

AWS Cloud Practitioner Essentials



Welcome to AWS Cloud Practitioner Essentials. In this course, you will learn about AWS Cloud concepts, AWS services, security, architecture, pricing, and support.

Course Overview



Agenda



- Introduction:** Course Overview
- Module 1:** Introduction to Amazon Web Services
- Module 2:** Compute in the Cloud
- Module 3:** Global Infrastructure and Reliability
- Module 4:** Networking
- Module 5:** Storage and Databases
- Module 6:** Security
- Module 7:** Monitoring and Analytics
- Module 8:** Pricing and Support
- Module 9:** Migration and Innovation
- Module 10:** AWS Certified Cloud Practitioner Basics

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

This course includes the following modules:

- 1: Introduction to Amazon Web Services
- 2: Compute in the Cloud
- 3: Global Infrastructure and Reliability
- 4: Networking
- 5: Storage and Databases
- 6: Security
- 7: Monitoring and Analytics
- 8: Pricing and Support
- 9: Migration and Innovation
- 10: AWS Certified Cloud Practitioner Basics

Introductions



- Name
- What you do for work
- What you hope to learn in this course
- What you like to do in your leisure time



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

4

Please introduce yourself by sharing the following details:

- Name
- What you do for work
- What you hope to learn in this course
- What you like to do in your leisure time

Module 1

Introduction to Amazon Web Services



Welcome to Module 1: Introduction to Amazon Web Services.

Module 1 objectives



In this module, you will learn how to:

- Describe three cloud computing deployment models
- Describe six benefits of cloud computing



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

6

In this module, you will learn how to:

- Describe three cloud computing deployment models
- Describe six benefits of cloud computing

Welcome to the coffee shop



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

7

Throughout this course, you will learn essential information about the breadth and depth of Amazon Web Services (AWS) offerings, and how AWS products and services can benefit companies. To help you understand some of these pieces, you will examine them through the metaphor of a coffee shop.

Almost all modern computing centers around a basic client-server model, which uses transactions similar to coffee shop transactions. In a coffee shop, a customer makes a request for a cup of coffee. This request is fulfilled when the barista prepares the order and provides it to the customer.

Client and server model



Client



A client makes a request.



Server



A server fulfills the client's request.

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

8

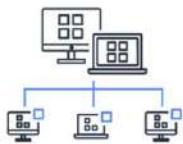
In computing, the “customer” is the client. A client can be a web browser or desktop application that a person interacts with to make a request to a computer server. The server is like the “barista” in the coffee shop. A server can be a service like Amazon Elastic Compute Cloud (Amazon EC2), a type of virtual server.

For example, suppose that a client requests a coffee order, coupons, promotions, and so on. The server evaluates the request and fulfills it by returning the information to the client.

Cloud computing



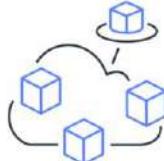
What is cloud computing?



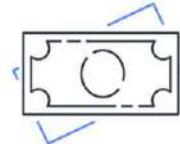
Access services on demand



Avoid large upfront investments



Provision computing resources as needed



Pay only for what you use

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

9

The client-server model enables **cloud computing**. Cloud computing refers to the on-demand delivery of IT resources and applications through the internet.

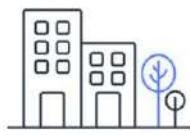
With cloud computing, you don't need to make large upfront investments in hardware, or spend time and resources managing hardware. Instead, you can provision exactly the right type and size of computing resources that you need to power your newest idea or operate your IT department. You can access as many resources as you need, and pay only for what you use.

This course begins by exploring principles and benefits of cloud computing. Then, you will examine a variety of AWS services that can be used for creating cloud-based applications and solutions.

Cloud computing deployment models



Cloud



On premises



Hybrid

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

10

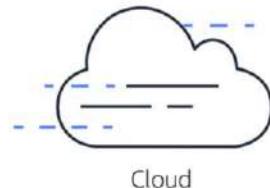
When selecting a cloud deployment strategy, a company must consider factors such as required cloud application components, preferred resource management tools, and legacy IT infrastructure requirements.

The three cloud computing deployment models are cloud-based, on-premises, and hybrid deployments.

Cloud-based deployment



- Run all parts of the application in the cloud
- Migrate existing applications to the cloud
- Design and build new applications in the cloud



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

11

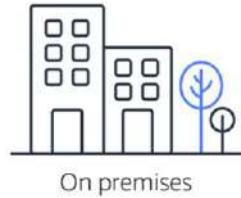
In a **cloud-based deployment** model, you can migrate existing applications to the cloud, or you can design and build new applications in the cloud. You can build the applications on low-level infrastructure that requires your IT staff to manage them. Or, you can build them using higher-level services that reduce the management, architecting, and scaling requirements of the core infrastructure.

For example, a company might create an application consisting of virtual servers, databases, and networking components that are fully based in the cloud. This would reduce the company's management, architecting, and scaling requirements.

On-premises deployment



- Use virtualization and resource management tools to deploy resources
- Use application management and virtualization technologies to increase resource usage



The second cloud computing deployment model is **on-premises deployment**.

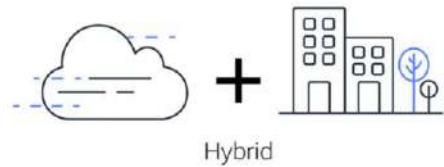
This is also known as a private cloud deployment. In this model, resources are deployed on premises by using virtualization and resource-management tools.

For example, you might have applications that run in your on-premises data center. While this model is like a legacy IT infrastructure, its incorporation of application management and virtualization technologies can help increase resource usage.

Hybrid deployment



- Connect cloud-based resources to on-premises infrastructure
- Integrate cloud-based resources with legacy IT applications



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

13

The third cloud computing deployment model is **hybrid deployment**.

In a hybrid deployment, cloud-based resources are connected to an on-premises infrastructure. You might want to use this approach in a number of situations. For example, you might have legacy applications that are better maintained on premises, or government regulations require your business to keep certain records on premises.

Suppose that a company wants to use cloud services that can automate batch data processing and analytics. However, the company has several legacy applications that are more suitable on premises and will not be migrated to the cloud. With a hybrid deployment, the company could keep the legacy applications on premises, and use the data and analytics services that run in the cloud.

Now that you have a general understanding of cloud computing, you will explore AWS Cloud offerings.

The screenshot shows the AWS Cloud Services console. At the top, there's a navigation bar with the AWS logo, a search bar, and links for 'Services', 'Explore AWS', 'Origins', and 'Support'. Below the navigation is a sidebar titled 'All services' with categories: Compute (EC2, Lightsail, Lambda, Batch, Elastic Beanstalk, Serverless Application Repository, AWS Outposts, EC2 Image Builder), Containers (Elastic Container Registry, Elastic Container Service, Elastic Kubernetes Service), Storage (S3, EFS, FSx, S3 Glacier, Storage Gateway, AWS Backup), and Database (RDS, DynamoDB). To the right of the sidebar is a main content area with several sections: 'Explore AWS' featuring 'Amazon Redshift', 'Run Serverless Containers with AWS Fargate', and 'Scalable, Durable, Secure Backup & Restore with Amazon S3'; 'AWS Marketplace' featuring 'Find, buy, and deploy popular software products that run on AWS'; and a 'Have feedback?' link. The bottom of the page includes a copyright notice for '© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.' and a page number '14'.

In 2006, AWS began offering IT infrastructure services to businesses as web services. This is now commonly known as cloud computing.

AWS services can be implemented for use cases across industries and businesses of varying sizes. These businesses include enterprises, startups, small- and medium-sized businesses, and AWS customers in the public sector. Even if you have not yet created your own AWS account, you have probably used applications that run in the AWS Cloud. Some examples of applications that run in the AWS Cloud include video streaming services, photo hosting applications, hotel reservation websites, and more.

The AWS Cloud is a comprehensive and broadly adopted cloud service. AWS offers more than 175 services from data centers globally. Some of the service categories included in the console are Compute, Containers, Storage, and Database. You do not need to know all the services. This course focuses on foundational concepts of the AWS Cloud. In the next section, you will explore some of the benefits of cloud computing.

Cloud computing benefits

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



As you begin to learn about cloud computing, also consider *why* a company might choose a particular cloud computing approach to address their business needs.

This section of the course explores six benefits of cloud computing. As you learn about each benefit, think about how you might have experienced the benefit at work or during other computing activities.

Variable expenses



Upfront expenses



Invest in technology resources before using them

Variable expenses



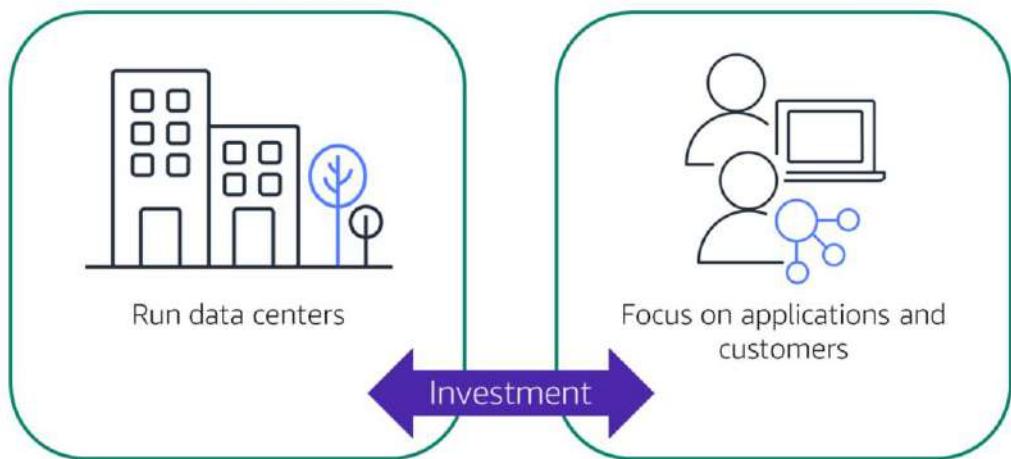
Pay only for what you use

With cloud computing, you can trade upfront expenses for variable expenses.

Upfront expenses refer to data centers, physical servers, and other resources that you invest in before using them. Variable expenses mean that you only pay for computing resources that you consume instead of investing heavily in data centers and servers before you know how you will use them.

By taking a cloud computing approach that offers the benefit of variable expenses, companies can implement innovative solutions while saving on costs.

Cost optimization



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

17

With cloud computing, you can optimize costs by no longer needing to spend money on running and maintaining data centers.

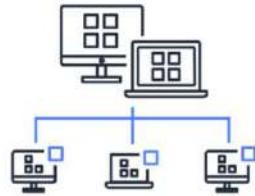
Computing in data centers often requires you to spend more money and time managing infrastructure and servers.

A benefit of cloud computing is the ability to focus less on those tasks and more on applications and customers.

Capacity



Stop guessing on your infrastructure capacity needs



Scale in and scale out as needed

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

18

You can stop guessing capacity.

With cloud computing, you don't have to predict how much infrastructure capacity you will need before deploying an application.

For example, you can launch Amazon EC2 instances when needed, and pay only for the compute time you use. Instead of paying for unused resources or dealing with limited capacity, you can access only the capacity that you need. You can scale in or scale out in response to demand.

Economies of scale

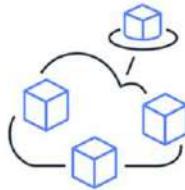


Smaller scale



Pay higher prices based on
only your own usage

Economies of scale



Benefit from customers'
aggregated usage

You can benefit from massive economies of scale.

By using cloud computing, you can achieve a lower variable cost than you can get on your own.

Because usage from hundreds of thousands of customers can aggregate in the cloud, AWS can achieve higher economies of scale. The economy of scale translates into lower pay-as-you-go prices.

Speed and agility



Data centers



Weeks between wanting resources and having resources

Cloud computing



Minutes between wanting resources and having resources

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

20

You can increase speed and agility.

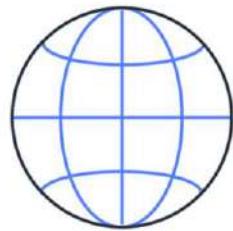
The flexibility of cloud computing makes it easier for you to develop and deploy applications. This flexibility provides you with more time to experiment and innovate.

When computing in data centers, it might take weeks to obtain new resources that you need. In comparison, cloud computing enables you to access new resources in minutes.

Global in minutes



Quickly deploy applications worldwide



Use the AWS global infrastructure.

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

21

You can go global in minutes.

The global footprint of the AWS Cloud enables you to deploy applications to customers around the world quickly, while providing them with low latency. This means that even if you are located in a different part of the world than your customers, customers can access your applications with minimal delays.

Later in this course, you will explore the AWS global infrastructure in greater detail. You will examine some of the services that you can use to deliver content to customers around the world.

AWS core service categories



Compute



Networking and Content Delivery



Storage



Database



Security, Identity,
and Compliance



Management
and Governance

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

22

Throughout this course, you will explore AWS services in categories such as:

- Compute
- Networking and Content Delivery
- Storage
- Database
- Security, Identity, and Compliance
- Management and Governance

As you begin to learn about AWS services, consider the features and benefits of a single service in addition to how you can potentially combine the services to offer a solution for your business needs.

For example, suppose that the owners of the coffee shop want to create a new application for customers. They might use the following types of services:

- Database service to store customer information
- Management and governance services to ensure that the application is designed in accordance with AWS best practices

- Networking and content delivery services to deliver websites and videos to customers

As a reminder, you do not need to know all the services that AWS offers. This course focuses on foundational concepts of the AWS Cloud.

Module 1

Knowledge check

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Knowledge check question 1



24

What is cloud computing?

- A. Backing up files that are stored on desktop and mobile devices to prevent data loss
- B. Deploying applications that are connected to an on-premises infrastructure
- C. Using on-demand delivery of IT resources and applications through the internet
- D. Running code without needing to manage or provision servers

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is cloud computing?

- A. Backing up files that are stored on desktop and mobile devices to prevent data loss
- B. Deploying applications that are connected to an on-premises infrastructure
- C. Using on-demand delivery of IT resources and applications through the internet
- D. Running code without needing to manage or provision servers

Knowledge check answer 1



25

What is cloud computing?

- A. Backing up files that are stored on desktop and mobile devices to prevent data loss
- B. Deploying applications that are connected to an on-premises infrastructure
- C. **Using on-demand delivery of IT resources and applications through the internet (correct)**
- D. Running code without needing to manage or provision servers

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **C. Using on-demand delivery of IT resources and applications through the internet.**

The other response options are incorrect because:

- A. While you can back up files to the cloud, this response option does not describe cloud computing as a whole.
- B. Response B describes a sample use case for a hybrid cloud deployment. Remember that cloud computing has cloud and on-premises (or private cloud) deployment models.
- D. AWS Lambda is an AWS service that lets you run code without needing to manage or provision servers. This description does not describe cloud computing as a whole. AWS Lambda is explained in greater detail in the next module.

Knowledge check question 2



26

What is another name for on-premises deployment?

- A. Cloud-based application
- B. Hybrid deployment
- C. Private cloud deployment
- D. AWS Cloud

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is another name for on-premises deployment?

- A. Cloud-based application
- B. Hybrid deployment
- C. Private cloud deployment
- D. AWS Cloud

Knowledge check answer 2



27

What is another name for on-premises deployment?

- A. Cloud-based application
- B. Hybrid deployment
- C. **Private cloud deployment (correct)**
- D. AWS Cloud

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **C. Private cloud deployment**.

The other response options are incorrect because:

- A. Cloud-based applications are fully deployed in the cloud and do not have any parts that run on premises.
- B. A hybrid deployment connects infrastructure and applications between cloud-based resources and existing resources that are not in the cloud, such as on-premises resources. However, a hybrid deployment is not equivalent to an on-premises deployment, because it involves resources that are located in the cloud.
- D – The AWS Cloud offers three cloud deployment models – cloud, hybrid, and on-premises. This response option is incorrect because the AWS Cloud is not equivalent to only on-premises deployment.

Knowledge check question 3



28

How does the scale of cloud computing help you save costs?

- A. You do not have to invest in technology resources before using them.
- B. The aggregated cloud usage from a large number of customers results in lower pay-as-you-go prices.
- C. Accessing services on-demand helps prevent excess or limited capacity.
- D. You can quickly deploy applications to customers and provide low latency.

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How does the scale of cloud computing help you save costs?

- A. You do not have to invest in technology resources before using them.
- B. The aggregated cloud usage from a large number of customers results in lower pay-as-you-go prices.
- C. Accessing services on-demand helps prevent excess or limited capacity.
- D. You can quickly deploy applications to customers and provide low latency.

Knowledge check answer 3



29

How does the scale of cloud computing help you save costs?

- A. You do not have to invest in technology resources before using them.
- B. **The aggregated cloud usage from a large number of customers results in lower pay-as-you-go prices. (correct)**
- C. Accessing services on-demand helps prevent excess or limited capacity.
- D. You can quickly deploy applications to customers and provide low latency.

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **B. The aggregated cloud usage from a large number of customers results in lower pay-as-you-go prices.** This answer describes how customers can benefit from massive economies of scale in cloud computing.

The other response options are incorrect because:

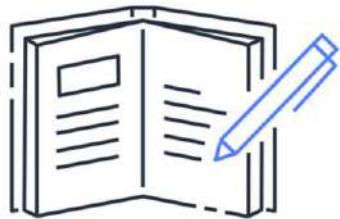
- A. This option relates to the concept of “trade upfront expense for variable expense.”
- C. This option relates to the concept of “stop guessing capacity.”
- D. This option relates to the concept of “go global in minutes.”

Module 1 summary



In this module, you learned about:

- Three cloud computing deployment models
- Six benefits of cloud computing



In this module, you learned about three cloud computing deployment models:

- Cloud
- On premises
- Hybrid

You also explored six benefits that cloud computing offers:

- Trade capital expenses for variable expenses
- Stop spending money running and maintaining data centers
- Stop guessing capacity
- Benefit from massive economies of scale
- Increase speed and agility
- Go global in minutes

With cloud computing, you can access services on demand, provision computing resources as needed, and save on costs by paying only for what you use.

The next module explores some of the compute services that AWS offers.

Module 2

Compute in the Cloud

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



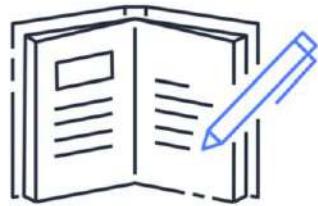
In this module, you will learn about Amazon Elastic Compute Cloud (Amazon EC2) instance types, pricing, and related services.

Module 2 objectives



In this module, you will learn how to:

- Describe Amazon EC2 benefits
- Identify the Amazon EC2 instance types
- Differentiate among Amazon EC2 billing options
- Summarize Amazon EC2 Auto Scaling benefits
- Summarize Elastic Load Balancing benefits
- Provide examples of Elastic Load Balancing uses
- Describe differences between Amazon SNS and Amazon SQS
- Summarize additional AWS compute options



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

32

In this module, you will learn how to:

- Describe Amazon Elastic Compute Cloud (Amazon EC2) benefits
- Identify the Amazon EC2 instance types
- Differentiate among Amazon EC2 billing options
- Summarize Amazon EC2 Auto Scaling benefits
- Summarize Elastic Load Balancing benefits
- Provide examples of Elastic Load Balancing uses
- Describe differences between Amazon Simple Notification Service (Amazon SNS) and Amazon Simple Queue Service (Amazon SQS)
- Summarize additional AWS compute options

Client and server model



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

53

To understand how computing works in the cloud, think about the client-server model introduced in the previous module. Companies use the client-server model to deliver products, resources, and data to their end users. This process is powered by computer servers that host applications and provide the compute power that businesses need.

In a coffee shop, a customer makes a request, and then, a barista fulfills the customer's request. Think of a barista as a virtual server that fulfills requests. A barista can fulfill requests by providing customers with items such as coffee, tea, or pastries. A virtual server can fulfill requests by providing a client with items such as videos, photos, or static webpages.

In AWS, you can use the Amazon EC2 service to run virtual servers.

Amazon Elastic Compute Cloud (Amazon EC2)

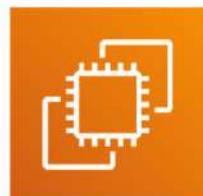
© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



Amazon EC2



- Use secure, sizable compute capacity
- Boot server instances in minutes
- Pay only for what you use



Amazon EC2

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

55

Amazon EC2 provides secure, resizable compute capacity in the cloud as Amazon EC2 instances.

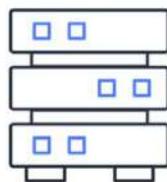
Imagine that you are responsible for the architecture of your company's resources and must support new websites. With traditional on-premises resources, you would:

1. Spend money upfront to purchase hardware.
2. Wait for the servers to be delivered to you.
3. Install the servers in your physical data center.
4. Make all the necessary configurations.

By comparison, with an Amazon EC2 instance, you would use a virtual server to run applications in the AWS Cloud. You could:

- Provision and launch an Amazon EC2 instance within minutes
- Stop using it when you finish running a workload
- Pay only for the compute time you use when an instance is running, not when it is stopped or shut down
- Save costs by paying only for server capacity that you need or want

How Amazon EC2 works



Launch an instance

Connect to the instance

Use the instance

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

36

Here is a quick summary of how Amazon EC2 works.

First, you launch an instance. To do this, you choose a template with basic configurations for your instance. These configurations include the operating system, application server, or applications. You also choose the instance type, which is the specific hardware configuration of your instance.

As you prepare to launch an instance, you specify security settings to control the network traffic that can flow in and out of your instance. Later in this course, you will explore Amazon EC2 security features in greater detail.

Next, connect to the instance. You can connect to the instance in several ways. Your programs and applications have multiple methods to connect directly to the instance and exchange data. Users can also connect to the instance by logging in and accessing the computer desktop.

After you connect to the instance, you can use it. You can run commands to install software, add storage, copy and organize files, and more.

Amazon EC2 instance types

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

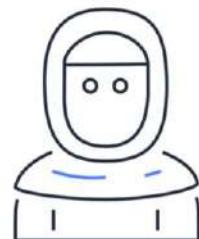


Amazon EC2 offers several instance types. This section focuses on what an instance type is and explores the various instance types that are available in Amazon EC2.

Coffee shop tasks



Employee 1



Employee 2



Employee 3



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

33

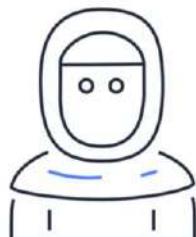
In a coffee shop, suppose that there is only one employee who does everything – makes coffee, processes transactions at the register, orders supplies, and so on. At each phase in the process, the customer ends up waiting. This would not be the most efficient use of resources or provide the best customer experience.

<click> Having several employees performing the same tasks would also not be efficient.

Coffee shop task specialization



Employee 1



Make coffee

Employee 2



Process transactions

Employee 3



Order supplies

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

59

Different employees have different strengths, such as designing creative latte art, quickly completing payment transactions, or tracking inventory. To keep the coffee shop running efficiently, you could let your employees specialize and work in their areas of strength.

Now, think of the coffee shop employees as different types of Amazon EC2 instances. You can launch Amazon EC2 instances in your AWS environment to complete different tasks.

AWS provides a broad choice of instances. They can be general purpose or optimized for specific needs, such as high performance computing, big data, storage, and analytics.

Amazon EC2 instance types



General purpose

- Balances compute, memory, and networking resources
- Suitable for a broad range of workloads

Compute optimized

- Offers high-performance processors
- Ideal for compute-intensive applications and batch processing workloads

Memory optimized

- Delivers fast performance for memory-intensive workloads
- Well suited for high-performance databases

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

40

When choosing an instance type, consider the specific needs of your workloads and applications. This might include requirements for compute, memory, or storage capabilities.

<click> General purpose instances provide a balance of compute, memory, and networking resources. They can be used for a variety of workloads, such as application servers, gaming servers, backend servers for enterprise applications, and small and medium databases.

Suppose that you have an application in which the resource needs for compute, memory, and networking are roughly equivalent. You might consider running it on a general purpose instance because the application does not require optimization in any single resource area.

<click> Compute optimized instances are ideal for compute-bound applications that benefit from high-performance processors. Like general purpose instances, compute optimized instances can be used for workloads such as web, application, and gaming servers.

However, the difference is that compute optimized applications are ideal for *high-performance* web servers, *compute-intensive* applications servers, and *dedicated* gaming servers. Compute optimized instances can also be used for batch processing workloads that require many transactions to be processed in a single group.

<click> Memory optimized instances are designed to deliver fast performance for workloads that process large datasets in memory. In computing, memory is a temporary storage area. It holds all the data and instructions that a central processing unit (CPU) needs to be able to complete actions. Before a computer program or application can run, it is loaded from storage into memory. This preloading process gives the CPU direct access to the computer program.

Suppose that you have a workload that requires large amounts of data to be preloaded before an application is run. This might be a high-performance database or a workload that involves performing real-time processing of big unstructured data. In these types of use cases, consider using a memory optimized instance. Memory optimized instances allow you to run workloads with high memory needs and receive great performance.

Accelerated computing

- Uses hardware accelerators to expedite data processing
- Ideal for application streaming and graphics workloads

Storage optimized

- Offers low latency and high input/output operations per second (IOPS)
- Suitable for workloads such as distributed file systems and data warehousing applications

Accelerated computing instances use hardware accelerators, or *coprocessors*, to perform some functions more efficiently than is possible in software running on CPUs. Examples of these functions include floating point number calculations, graphics processing, and data pattern matching.

In computing, a hardware accelerator is a component that can expedite data processing. Accelerated computing instances are ideal for workloads such as graphics applications, game streaming, and application streaming.

<click> Storage optimized instances are designed for workloads that require high, sequential read and write access to large datasets on local storage. Examples of workloads suitable for storage optimized instances include distributed file systems, data warehousing applications, and high-frequency online transaction processing (OLTP) systems.

In computing, input/output operations per second (IOPS) is a metric that measures the performance of a storage device. It indicates how many different input or output operations a device can perform in one second. Storage optimized instances are designed to deliver tens of thousands of low-latency, random IOPS to applications.

You can think of input operations as data that is put into a system, such as records that are entered into a database. Output operations are data that is generated by a server. An example of output might be the analytics that are performed on the records in a database. If you have an application that has a high IOPS requirement, a storage optimized instance can potentially provide improved performance over other instance types that are not optimized for this kind of use case.

Reference

- For more information about Amazon EC2 instance types, review “Amazon EC2 Instance Types” at: [https://aws.amazon.com/ec2\(instance-types/](https://aws.amazon.com/ec2(instance-types/)

Match: Amazon EC2 instance types



1. Ideal for high-performance databases

A. General purpose

2. Suitable for data warehousing applications

B. Compute optimized

3. Balances compute, memory, and networking resources

C. Memory optimized

4. Offers high-performance processors

D. Storage optimized

Before moving to the next topic, take a moment to review some descriptions and use cases for the Amazon EC2 instance types. This activity involves matching each option on the left to an Amazon EC2 instance type on the right.

First, which Amazon EC2 instance type is ideal for high-performance databases?

Match: Amazon EC2 instance types



1. Ideal for high-performance databases

A. General purpose

2. Suitable for data warehousing applications

B. Compute optimized

3. Balances compute, memory, and networking resources

C. Memory optimized

4. Offers high-performance processors

D. Storage optimized

Memory optimized instances are ideal for high-performance databases.

Which Amazon EC2 instance type is suitable for data warehousing applications?

Match: Amazon EC2 instance types



1. Ideal for high-performance databases

2. Suitable for data warehousing applications

3. Balances compute, memory, and networking resources

4. Offers high-performance processors

A. General purpose

B. Compute optimized

C. Memory optimized

D. Storage optimized

Storage optimized instances are suitable for data warehousing applications.

Which Amazon EC2 instance type balances compute, memory, and networking resources?

Match: Amazon EC2 instance types



1. Ideal for high-performance databases

2. Suitable for data warehousing applications

3. Balances compute, memory, and networking resources

4. Offers high-performance processors

A. General purpose

B. Compute optimized

C. Memory optimized

D. Storage optimized

General purpose instances balance compute, memory, and networking resources.

Which Amazon EC2 instance type offers high-performance processors?

Match: Amazon EC2 instance types



1. Ideal for high-performance databases

A. General purpose

2. Suitable for data warehousing applications

B. Compute optimized

3. Balances compute, memory, and networking resources

C. Memory optimized

4. Offers high-performance processors

D. Storage optimized

Compute optimized instances offer high-performance processors.

Next is a review of the Amazon EC2 pricing options.

Amazon EC2 pricing

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



So far in this module, you have examined the Amazon EC2 instance types. This section describes the Amazon EC2 pricing.

Additional AWS pricing tools and services are explained later in this course.

Amazon EC2 instance pricing options



On-Demand

- No upfront costs or minimum contracts
- Ideal for short-term, irregular workloads

Spot

- Ideal for workloads with flexible start and end times
- Offers savings over On-Demand prices

With Amazon EC2, you pay only for the compute time that you use. Amazon EC2 offers a variety of pricing options for different use cases.

In the coffee shop example, suppose that the owners are experimenting with a new application that is still in the development and testing phases. The application does not yet need to run for long periods of time. However, when the application does run, it must do so without interruption so its performance can be accurately assessed.

On-Demand Instances are an excellent option to use for this type of short-term, irregular workload that cannot be interrupted. No upfront costs or minimum contracts apply. The instances run continuously until you stop them, and you pay for only the compute time you use.

Sample use cases for On-Demand Instances include developing and testing applications, and running applications that have unpredictable usage patterns. On-Demand Instances are not recommended for workloads that last a year or longer, because these workloads can experience greater cost savings through the use of Reserved Instances.

<click> The owners of the coffee shop might also use an Amazon EC2 instance for their data processing, such as a batch workload that aggregates and analyzes customer survey data. Compared to other types of batch workloads in the coffee shop, such as daily financial processing, the survey data processing is not mission-critical. To save costs, the coffee shop owners decide to use a Spot Instance for their survey data processing.

Spot Instances are ideal for these types of workloads with flexible start and end times, or that can withstand interruptions. Spot Instances use unused EC2 computing capacity and offer you cost savings at up to 90 percent of On-Demand prices.

Suppose that you have a background processing job that can start and stop as needed (such as the customer survey data processing job). You want to start and stop the processing job without affecting the overall operations of your business. If you make a Spot request and Amazon EC2 capacity is available, your Spot Instance launches. However, if you make a Spot request and Amazon EC2 capacity is unavailable, the request is not successful until capacity becomes available. The unavailable capacity might delay the launch of your background processing job.

After you have launched a Spot Instance, if capacity is no longer available or demand for Spot Instances increases, your instance might be interrupted. This might not pose any issues for your background processing job. However, in the earlier example of developing and testing applications, you would most likely want to avoid unexpected interruptions. Therefore, you should choose a different EC2 instance type that is more ideal for those tasks.

Amazon EC2 instance pricing options



Reserved

- Provides a billing discount over On-Demand pricing
- Requires a 1-year or 3-year term commitment

Compute Savings Plan

- Offers up to 72% savings over On-Demand costs for a consistent amount of compute usage
- Requires a 1-year or 3-year term commitment

Suppose that the coffee shop owners have an application that will run continuously for at least a year. An example of this might be the main application that customers use for mobile ordering. The owners don't think that Spot Instances would be a good fit because of possible interruptions. They also considered On-Demand Instances, but the estimated price seems high for what they would pay for a year of compute time. This is an example of when to consider **Reserved Instances**.

Reserved Instances are a billing discount that is applied to the use of On-Demand Instances in your account. You can purchase Standard Reserved and Convertible Reserved Instances for a 1-year or 3-year term, and Scheduled Reserved Instances for a 1-year term. You realize greater cost savings with the 3-year option.

At the end of a Reserved Instance term, you can continue using the EC2 instance without interruption. However, you are charged On-Demand rates until you shut down the instance or purchase a new Reserved Instance that matches the instance attributes (instance type, Region, tenancy, and platform).

Next, suppose that the coffee shop owners want to save costs on their EC2 compute usage, but they want to have even more flexibility than what is possible with

Reserved Instances. In this situation, they might consider purchasing a **Compute Savings Plan**.

AWS offers Savings Plans for several compute services, including Amazon EC2. Amazon EC2 Savings Plans can help you reduce your compute costs by committing to a consistent amount of compute usage for a 1-year or 3-year term. This results in savings of up to 72 percent over On-Demand costs.

Any usage up to the commitment is charged at the discounted Savings Plan rate (for example, \$10 an hour). Any usage beyond the commitment is charged at regular On-Demand rates.

Later in this course, you will review AWS Cost Explorer, a tool that can help you visualize, understand, and manage your AWS costs and usage over time. If you are considering your options for Savings Plans, AWS Cost Explorer can analyze your EC2 usage over the past 7, 30, and 60 days. AWS Cost Explorer also provides customized recommendations for Savings Plans. These recommendations estimate how much you could save on your monthly EC2 costs, based on previous EC2 usage and the hourly commitment amount in a 1-year or 3-year Savings Plan.

For more information on Savings Plans, please visit
<https://aws.amazon.com/savingsplans/pricing/>.

Dedicated Instance

- An EC2 *instance* that runs in a VPC on hardware for a single customer
- Higher cost compared to standard Amazon EC2 instances

Dedicated Host

- A *physical server* with EC2 instance capacity for a single customer
- Most expensive Amazon EC2 option

Now, suppose that there is a healthcare clinic located next to the coffee shop. The clinic must meet specific compliance and regulatory requirements. For example, it must ensure that its data doesn't reside on the same data servers that are used by other companies. Dedicated Instances and Dedicated Hosts are two options to consider for these types of use cases.

- <click> **Dedicated Instances** are EC2 instances that run in a virtual private cloud (VPC) on hardware that is dedicated to a single customer. Dedicated Instances have a higher cost compared to standard Amazon EC2 instances. Dedicated Instances run uninterrupted, and you pay for only the compute time you use. However, you also have the option to reduce your costs by purchasing Reserved Dedicated Instances.
- <click> **Dedicated Hosts** are physical servers with EC2 instance capacity that is fully dedicated to your use. You can use your existing per-socket, per-core, or per-VM software licenses to help maintain license compliance. You can purchase Dedicated Hosts on-demand or reserved. Of all the EC2 options covered, Dedicated Hosts are the most expensive.

Knowledge check question



51

What is the difference between Compute Savings Plans and Spot Instances?

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Knowledge checks are used throughout this course to review concepts. These are usually services or concepts that seem similar but are different in meaning or function.

For this knowledge check, consider the Amazon EC2 instance pricing options. What is the difference between Compute Savings Plans and Spot Instances?

Knowledge check answer



52

- Compute Savings Plans are ideal for workloads that involve a consistent amount of compute usage over a 1-year or 3-year term.
- Spot Instances are ideal for workloads with flexible start and end times, or that can withstand interruptions.

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

- **Compute Savings Plans** are ideal for workloads that involve a consistent amount of compute usage over a 1-year or 3-year term. With Compute Savings Plans, you can reduce your compute costs by up to 72 percent over On-Demand costs.
- **Spot Instances** are ideal for workloads with flexible start and end times, or that can withstand interruptions. Unlike Amazon EC2 Savings Plans, Spot Instances do not require contracts or a commitment to a consistent amount of compute usage.

Amazon EC2 Auto Scaling

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



This section explores Amazon EC2 Auto Scaling.

Manual scaling



Low demand



Customers



Barista

High demand



Customers



Baristas

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

54

Suppose that in the coffee shop, a barista is assigned to work at the register. When the coffee shop is in a period of low demand, the barista can readily manage their workload.

<click> Now, suppose that the coffee shop is open during its busiest season of the year. Because of the increased demand, the barista feels overwhelmed by the increased workload.

<click> The barista asks the manager for additional assistance, and the manager assigns another barista to help. When the workload decreases, the second barista can stop working at the register. This process is an example of *manual scaling*.

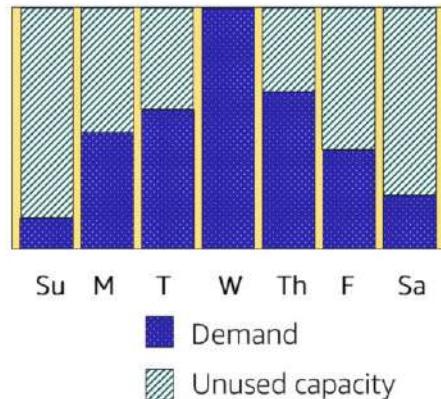
Scalability involves beginning with only the resources you need and designing your architecture to scale automatically in and out in response to changing demands. As a result, you pay for only the resources you use. You don't have to worry about a lack of computing capacity to meet your customers' needs.

What if you want scaling to happen automatically? The AWS service that provides this functionality for Amazon EC2 instances is **Amazon EC2 Auto Scaling**.

Amazon EC2 Auto Scaling



- Scale capacity as computing requirements change
- Use dynamic scaling and predictive scaling



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

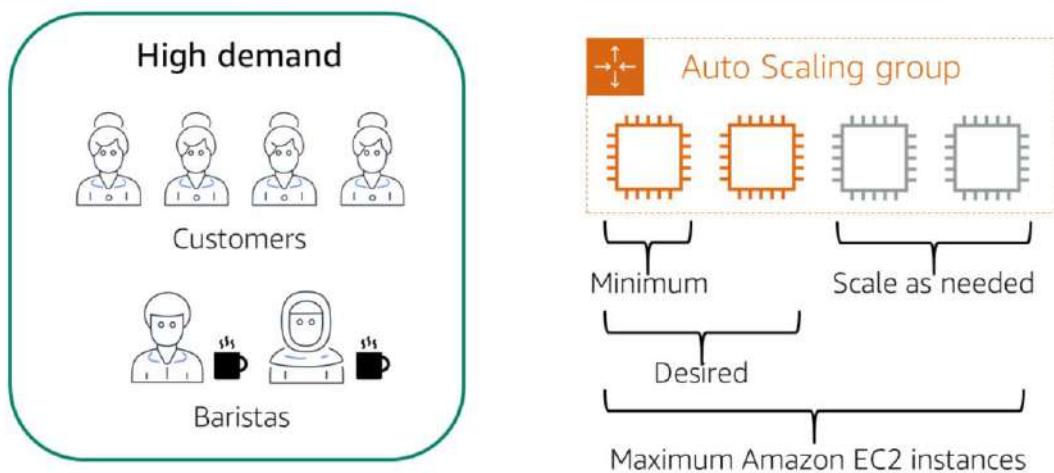
55

Have you ever tried to access a website that wouldn't load and it kept timing out? The website might have been receiving more requests than it was able to handle. This is similar to the experience of waiting in a long line at a coffee shop, when there is only one barista present to take orders from customers.

Amazon EC2 Auto Scaling can help you automatically add or remove Amazon EC2 instances in response to changing application demand. By automatically scaling your instances in and out as needed, you can maintain a greater sense of application availability.

With Amazon EC2 Auto Scaling, you can use two approaches – dynamic scaling and predictive scaling. *Dynamic scaling* responds to changing demand. *Predictive scaling* automatically schedules the right number of Amazon EC2 instances based on predicted demand. To scale faster, you can use dynamic scaling and predictive scaling together.

Amazon EC2 Auto Scaling (cont.)



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

56

In the cloud, computing power is a programmatic resource, so you can take a more flexible approach to the issue of scaling. By adding Amazon EC2 Auto Scaling to an application, you can add new instances to the application when necessary and remove them when no longer needed.

Suppose that you are preparing to run an application on Amazon EC2 instances. When configuring the size of your Auto Scaling group, you might set the minimum number of Amazon EC2 instances at one. This means that at all times, at least one Amazon EC2 instance must be running.

When you create an Auto Scaling group, you can set the minimum number of Amazon EC2 instances. The **minimum capacity** is the number of Amazon EC2 instances that launch immediately after you create the Auto Scaling group. In this example, the Auto Scaling group has a minimum capacity of one Amazon EC2 instance.

Next, you can set the **desired capacity** at two Amazon EC2 instances, even though your application needs a minimum of a single Amazon EC2 instance to run. If you do not specify the desired number of Amazon EC2 instances in an Auto Scaling group, the desired capacity defaults to your minimum capacity.

The third configuration that you can set in an Auto Scaling group is the **maximum capacity**. For example, you might configure the Auto Scaling group to scale out in response to increased demand, but only to a maximum of four Amazon EC2 instances.

Because Amazon EC2 Auto Scaling uses Amazon EC2 instances, you pay for only the instances you use, when you use them. You now have a cost-effective architecture that provides the best customer experience while reducing expenses.

Elastic Load Balancing

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

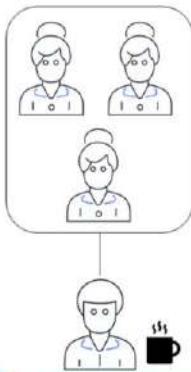


This section explores how you can distribute your application's workload by using Elastic Load Balancing.

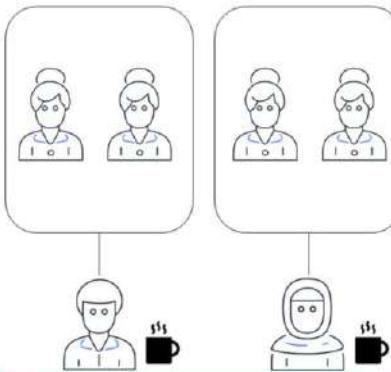
Load balancing



Unbalanced workload



Balanced workload



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

58

Using the previous example in the coffee shop, suppose that only one barista is doing the majority of the work and is overworked, while the other barista is underworked.

<click> To prevent any barista from becoming overwhelmed, the workload can be redistributed so that both baristas will serve the same number of customers.

Spreading workloads improves the performance of your applications by preventing any single resource from having to handle the full workload on its own. In this example, the number of customers remains the same, but balancing the workload evenly distributes the customers across the two baristas.

With **Elastic Load Balancing** in AWS, the size of a workload remains the same, but the workload is balanced by evenly distributing it across Amazon EC2 instances.

Elastic Load Balancing



- Automatically distributes traffic across multiple resources
- Provides a single point of contact for your Auto Scaling group



Elastic Load Balancing

Elastic Load Balancing is the AWS service that automatically distributes incoming application traffic across multiple resources, such as Amazon EC2 instances.

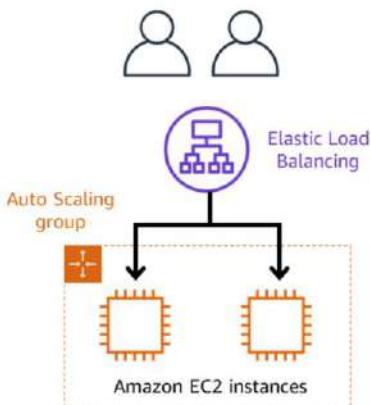
A load balancer acts as a single point of contact for all incoming web traffic to your Auto Scaling group. This means that as EC2 instances are added or removed in response to the amount of incoming traffic, these requests are routed to the load balancer first. Then, they are spread across multiple resources that will handle them. For example, if your application has been configured to have multiple EC2 instances, Elastic Load Balancing distributes the workload across the multiple instances so that no single instance has to carry the bulk of it.

Although Elastic Load Balancing and Amazon EC2 Auto Scaling are separate services, they work together to help ensure that applications running in Amazon EC2 can provide high performance and availability.

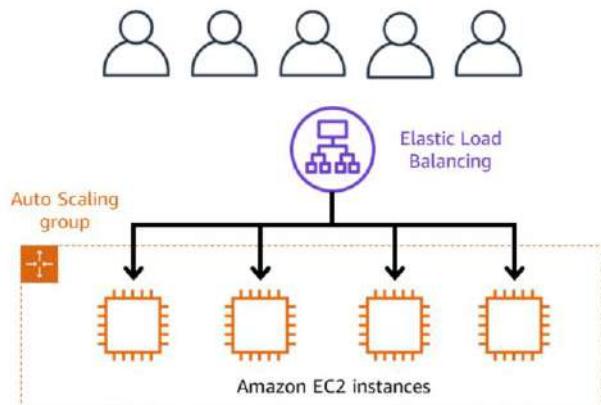
Scalability and load balancing



Low-demand period



High-demand period



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

60

Here's an example of how Elastic Load Balancing works. Suppose that a few customers have come to the coffee shop and are ready to place their orders. If only a few registers are open, this matches the demand of customers who need to be served. The coffee shop will be less likely to have open registers with no customers. In this example, you can think of the registers as Amazon EC2 instances.

Throughout the day, as the number of customers increases, the coffee shop opens more registers to accommodate them. In the diagram, this is represented by the Auto Scaling group.

Additionally, a coffee shop employee directs customers to the most appropriate register so that the number of requests can be evenly distributed across the open registers. You can think of this coffee shop employee as a load balancer.

Auto Scaling and Elastic Load Balancing



Are these examples of Auto Scaling or Elastic Load Balancing?

Auto Scaling

1. Removes unneeded Amazon EC2 instances when demand is low

Elastic Load Balancing

3. Distributes a workload across several Amazon EC2 instances

Auto Scaling

5. Automatically adjusts the number of Amazon EC2 instances to match demand

2. Adds a second Amazon EC2 instance during an online store's popular sale

Auto Scaling

4. Ensures that no single EC2 instance has to carry the full workload on its own

Elastic Load Balancing

6. Provides a single point of contact for traffic into an Auto Scaling group

Elastic Load Balancing

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

61

Instructor notes

This is a quick quiz to engage participants and test their understanding of the differences between Auto Scaling and Elastic Load Balancing. If they get any answer wrong, use the opportunity to further clarify why the answer is incorrect.

Click once for each question and answer. Review whether each is an example of Auto Scaling or Elastic Load Balancing. Items that are filled in with purple are examples of Auto Scaling; those that are filled in with green are examples of Elastic Load Balancing. Additionally, the label that appears next to each example indicates whether it is an example of Auto Scaling or Elastic Load Balancing.

AWS messaging services

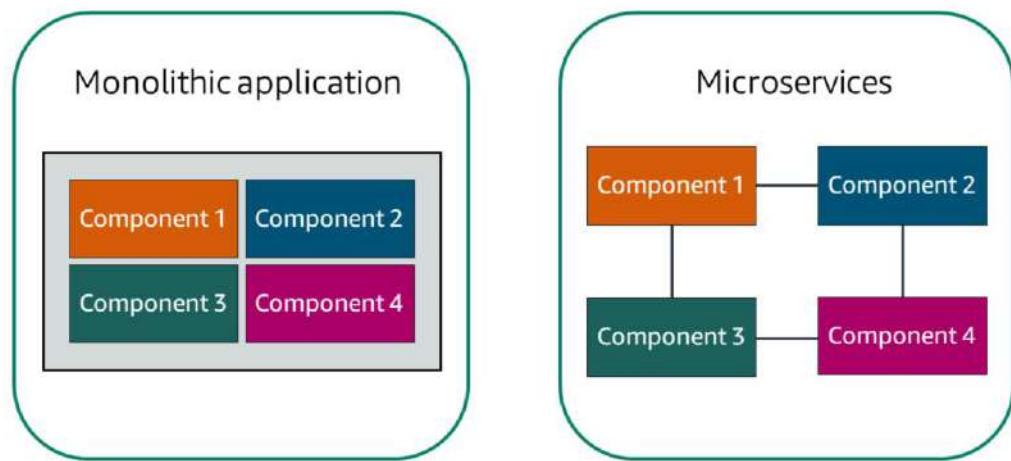
© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



You now have an understanding of how communication occurs between elastic load balancers and Amazon EC2 instances. What if you want to send data or messages between various AWS services and components?

This section explores AWS messaging services.

Application architecture



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

63

Applications are made of multiple components. The components communicate with each other to transmit data, fulfill requests, and keep the application running.

Suppose that you have an application with tightly coupled components. These components might include databases, servers, the user interface, business logic, and so on. This type of architecture can be considered a **monolithic application**. In this approach to application architecture, if a single component fails, other components fail, and possibly the entire application fails.

To help maintain application availability when a single component fails, you can design your application through a **microservices** approach. In a microservices approach, application components are loosely coupled. In this case, if a single component fails, the other components continue to work because they are communicating with each other. The loose coupling prevents the entire application from failing.

When designing applications on AWS, you can take a microservices approach with services and components that fulfill different functions. Two services facilitate application integration: Amazon Simple Notification Service (Amazon SNS) and

Amazon Simple Queue Service (Amazon SQS).

Amazon Simple Notification Service



- Messages are published to topics.
- Subscribers immediately receive messages for their topics.



Amazon Simple
Notification Service
(Amazon SNS)

Amazon Simple Notification Service (Amazon SNS) is a publish/subscribe service. Using Amazon SNS topics, a publisher publishes messages to subscribers. This is similar to how in the coffee shop, the cashier provides coffee orders to the barista who makes the drinks.

In Amazon SNS, subscribers can be web servers, email addresses, AWS Lambda functions, or several other options.

AWS Lambda is explained in more detail later in this module.

Publish updates from a single topic



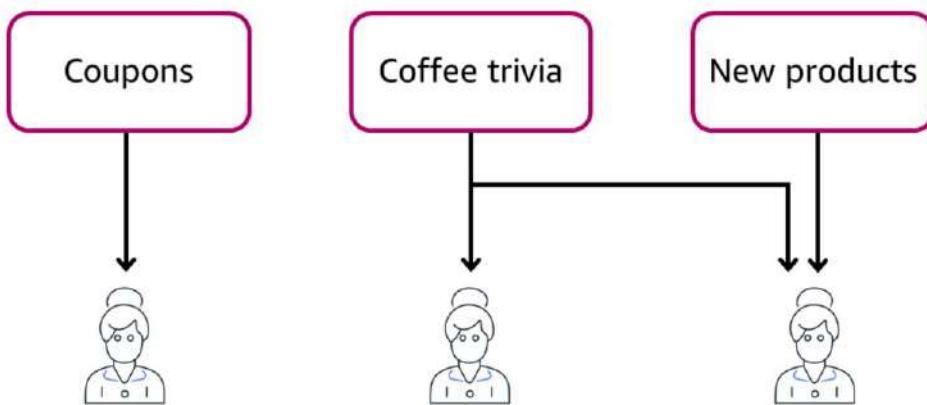
Coupons, coffee trivia, and new products



Here's an example that can help you understand how Amazon SNS works. Suppose that the coffee shop has a single newsletter that includes updates from all areas of its business, including topics such as coupons, coffee trivia, and new products. Because this is a single newsletter, coupons, coffee trivia, and new products are grouped into a single topic. All customers who subscribe to the newsletter receive updates about coupons, coffee trivia, and new products.

After a while, some customers begin to express that they would prefer to receive separate newsletters for only the specific topics that interest them. The coffee shop owners decide to try this approach.

Publish updates from multiple topics



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

56

Now, instead of having a single newsletter for all topics, the coffee shop has three separate newsletters. Each newsletter is devoted to a specific topic – coupons, coffee trivia, or new products.

Compared to the single newsletter with all topics, subscribers can now receive updates for only the specific topics to which they subscribe. Updates for topics are immediately sent to subscribers.

Subscribers can subscribe to a single topic or multiple topics. For example, the first customer is subscribed to only the coupons topic, and the second subscriber is subscribed to only the coffee trivia topic. The third customer is subscribed to both the coffee trivia and new products topics.

Although this example from the coffee shop involves subscribers who are people, in Amazon SNS, subscribers can be web servers, email addresses, AWS Lambda functions, or several other options.

Amazon Simple Queue Service



- Send, store, and receive messages between software components
- Queue messages without requiring other services to be available

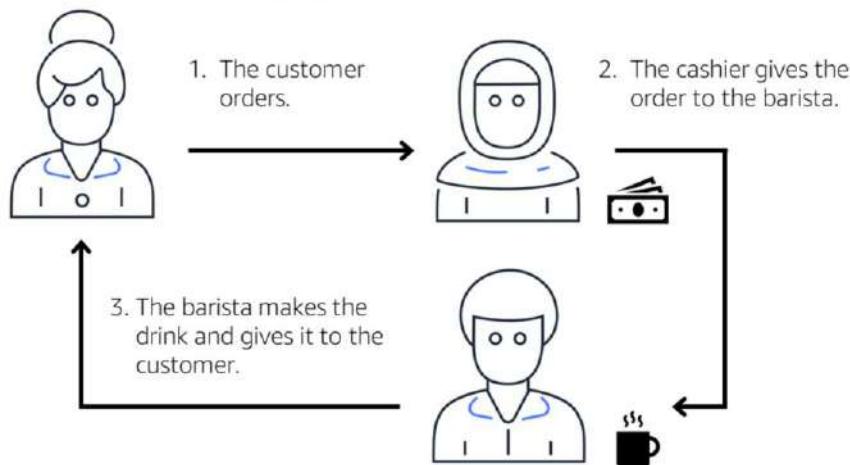


Amazon Simple Queue Service (Amazon SQS)

Next, Amazon Simple Queue Service (Amazon SQS) is a message queuing service.

Using Amazon SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available. In Amazon SQS, an application sends messages into a queue. A user or service retrieves a message from the queue, processes it, and then deletes it from the queue.

Example: Fulfill an order



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

68

Here's an example of how Amazon SQS works. Suppose that the coffee shop has an ordering process in which a cashier takes orders and a barista makes the orders. Think of the cashier and the barista as two separate components of an application.

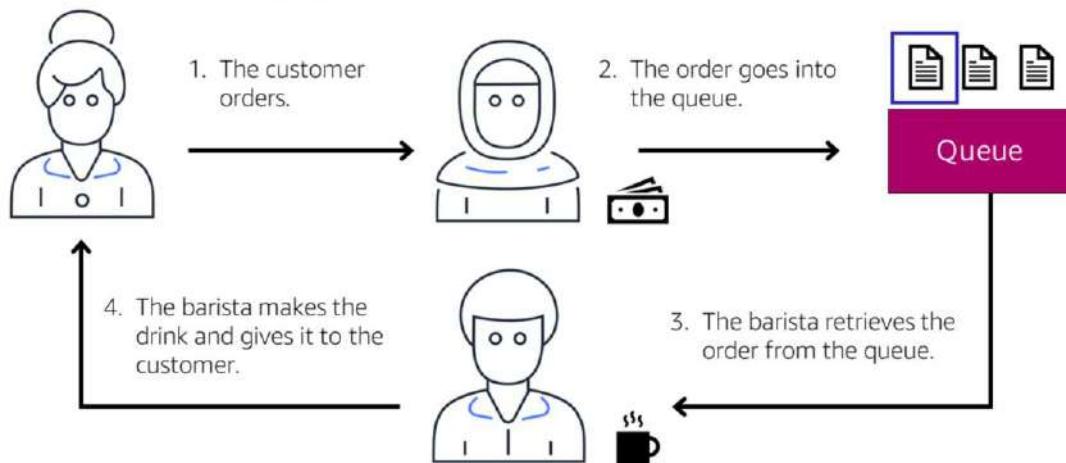
First, the cashier takes an order and writes it down on a piece of paper. Next, the cashier delivers the paper to the barista. Finally, the barista makes the drink and gives it to the customer.

When the next order comes in, the process repeats. This process runs smoothly as long as both the cashier and the barista are coordinated.

What might happen if the cashier took an order and went to deliver it to the barista, but the barista was out on a break or busy with another order? The cashier would need to wait until the barista is ready to accept the order. This would cause delays in the ordering process and require customers to wait longer to receive their orders.

As the coffee shop has become more popular and the ordering line is moving more slowly, the owners notice that the current ordering process is time consuming and inefficient. They decide to try a different approach that uses a queue.

Example: Orders in a queue



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

10

Recall that the cashier and the barista are two separate components of an application. A message queuing service such as Amazon SQS enables messages between decoupled application components.

In this example, the first step in the process remains the same as before – a customer places an order with the cashier.

The cashier puts the order into a queue. You can think of this as an order board that serves as a buffer between the cashier and the barista. Even if the barista is out on a break or busy with another order, the cashier can continue placing new orders into the queue.

Next, the barista checks the queue and retrieves the order.

The barista prepares the drink and gives it to the customer.

The barista then removes the completed order from the queue.

While the barista is preparing the drink, the cashier is able to continue taking new

orders and add them to the queue.

Serverless compute services

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

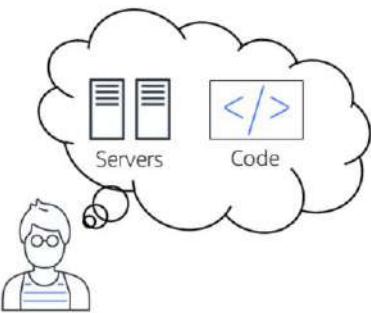


In the next section, you will learn about serverless compute services. As with messaging services, serverless compute services can also be used for innovating in your applications that run on AWS.

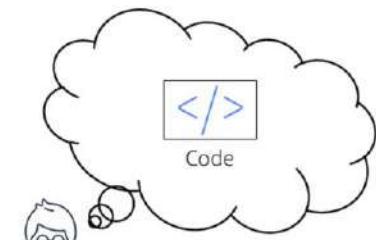
Serverless computing



Computing with virtual servers



Serverless computing



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

71

Earlier in this module, you learned about Amazon EC2, a service that lets you run virtual servers in the cloud. If you have applications that you want to run in Amazon EC2, you must do the following:

1. Provision instances (virtual servers).
2. Upload your code.
3. Continue to manage the instances while your application is running.

<click> In AWS, you can also build and run serverless applications. The term *serverless* means that your code runs on servers, but you do not need to provision or manage the servers. With serverless computing, you can focus more on innovating new products and features, instead of maintaining servers.

Another benefit of serverless computing is the flexibility to scale serverless applications automatically or to adjust their capacity by modifying the units of consumptions, such as throughput and memory.

An AWS service for serverless computing is AWS Lambda.

- Run code without provisioning or managing servers
- Pay only for compute time while code is running
- Use other AWS services to automatically trigger code



AWS Lambda

AWS Lambda is a service that lets you run code without needing to provision or manage servers.

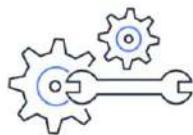
While using AWS Lambda, you pay only for the compute time that you consume. Charges apply only when your code is running. You can also run code for virtually any type of application or backend service, all with zero administration.

For example, a simple Lambda function might involve automatically resizing uploaded images to the AWS Cloud. In this case, the function triggers when uploading a new image.

How AWS Lambda works



Upload code to Lambda.



Set code to trigger from an event source.



Code runs only when triggered.



Pay only for the compute time you use.

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

73

Here's a brief overview of how AWS Lambda works.

First, you upload your code to Lambda. Next, you set your code to trigger from an event source, such as AWS services, mobile applications, or HTTP endpoints. Lambda runs your code only when triggered, and you pay only for the compute time that you use.

In the previous example of resizing images, you would pay only for the compute time that you use when new images are uploaded. Uploading the images triggers Lambda to run code for the image resizing function.

AWS container services

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

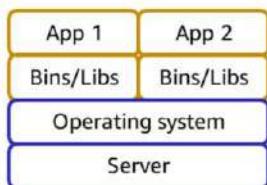


AWS also offers services that you can use to run containerized applications. In the next section, you will learn about containers and three AWS container services.

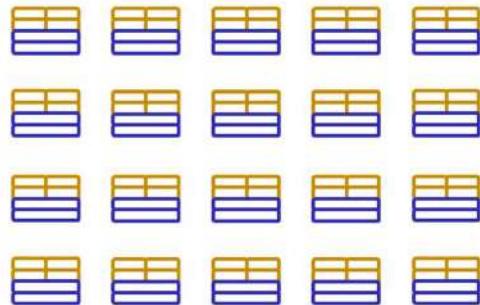
Containers



One host with multiple containers



Tens of hosts with hundreds of containers



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

75

Containers provide you with a standard way to package your application's code and dependencies into a single object. Containers are frequently used for processes and workflows in which there are essential requirements for security, reliability, and scalability.

Suppose that a company's application developer has an environment on their computer that is different from the environment on the computers used by the IT operations staff. The developer wants to ensure that the application's environment remains consistent regardless of where it is deployed, so they use a containerized approach. This helps reduce the time spent debugging applications and diagnosing differences in computing environments.

<click> When running containerized applications, you must consider scalability. Suppose that instead of a single host with multiple containers, you have to manage tens of hosts with hundreds of containers. Alternatively, you have to manage possibly hundreds of hosts with thousands of containers. At a large scale, imagine how much time it might take for you to monitor memory usage, security, logging, and so on.

Container orchestration services help you to deploy, manage, and scale your

containerized applications. You will learn about two services that provide container orchestration – Amazon Elastic Container Service (Amazon ECS) and Amazon Elastic Kubernetes Service (Amazon EKS).

AWS container orchestration services



Amazon Elastic
Container Service
(Amazon ECS)

- Run and scale containerized applications
- Use simple API calls to control Docker-enabled applications



Amazon Elastic
Kubernetes Service
(Amazon EKS)

- Run and scale Kubernetes applications
- Readily update applications with new features

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

76

Amazon Elastic Container Service (Amazon ECS) is a highly scalable, high-performance container management system that allows you to run and scale containerized applications on AWS.

Amazon ECS supports Docker containers. Docker is a software platform that allows you to build, test, and deploy applications quickly. AWS supports the use of open-source Docker Community Edition and subscription-based Docker Enterprise Edition. With Amazon ECS, you can use API calls to launch and stop Docker-enabled applications.

<click> Amazon Elastic Kubernetes Service (Amazon EKS) is a fully managed service that you can use to run Kubernetes on AWS.

Kubernetes is open source software that allows you to deploy and manage containerized applications at scale. Kubernetes is maintained by a large community of volunteers, and AWS actively works with the Kubernetes community. As new features and functionalities for Kubernetes applications are released, you can apply these updates to your applications that are managed with Amazon EKS.

AWS Fargate



- Run serverless containers with Amazon ECS or Amazon EKS
- Pay only for the resources you use



AWS Fargate

AWS Fargate is a serverless compute engine for containers. It works with both Amazon ECS and Amazon EKS. Unlike Amazon ECS and Amazon EKS, which are both container orchestration services, AWS Fargate is a container hosting platform.

When using AWS Fargate, you do not need to provision or manage servers. AWS Fargate manages your server infrastructure for you. You can focus more on innovating and developing your applications, and you pay only for the resources that are required to run your containers.

Module 2

Knowledge check

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



Knowledge check question 1



79

A customer wants to use an Amazon EC2 instance for a batch processing workload. Which Amazon EC2 instance type should they use?

- A. General purpose
- B. Compute optimized
- C. Memory optimized
- D. Storage optimized

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

A customer wants to use an Amazon EC2 instance for a batch processing workload. Which Amazon EC2 instance type should they use?

- A. General purpose
- B. Compute optimized
- C. Memory optimized
- D. Storage optimized

Knowledge check answer 1



80

A customer wants to use an Amazon EC2 instance for a batch processing workload. Which Amazon EC2 instance type should they use?

- A. General purpose
- B. Compute optimized (correct)**
- C. Memory optimized
- D. Storage optimized

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **B. Compute optimized**.

The other response options are incorrect because:

- A. General purpose instances provide a balance of compute, memory, and networking resources. This instance family would not be an ideal choice for the application in this scenario. Compute optimized instances are more suited for batch processing workloads than general purpose instances.
- C. Memory optimized instances are more ideal for workloads that process large datasets in memory, such as high-performance databases.
- D. Storage optimized instances are designed for workloads that require high, sequential read and write access to large datasets on local storage. The question does not specify the size of data that will be processed. Batch processing involves processing data in groups. A compute optimized instance is ideal for this type of workload, which would benefit from a high-performance processor.

Knowledge check question 2



81

What are the contract length options for Amazon EC2 Reserved Instances? (Select TWO.)

- A. 1 year
- B. 2 years
- C. 3 years
- D. 4 years
- E. 5 years

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

What are the contract length options for Amazon EC2 Reserved Instances? (Select TWO.)

- A. 1 year
- B. 2 years
- C. 3 years
- D. 4 years
- E. 5 years

Knowledge check answer 2



82

What are the contract length options for Amazon EC2 Reserved Instances? (Select TWO.)

- A. 1 year (correct)
- B. 2 years
- C. 3 years (correct)
- D. 4 years
- E. 5 years

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The two correct response options are:

- A. 1 year**
- C. 3 years**

Reserved Instances require a commitment of either 1 year or 3 years. The 3-year option offers a larger discount.

Knowledge check question 3



83

A customer has a workload that will run for a total of 6 months and can withstand interruptions. What would be the most cost-efficient Amazon EC2 instance purchasing option?

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

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

A customer has a workload that will run for a total of 6 months and can withstand interruptions. What would be the most cost-efficient Amazon EC2 instance purchasing option?

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

Knowledge check answer 3



84

A customer has a workload that will run for a total of 6 months and can withstand interruptions. What would be the most cost-efficient Amazon EC2 instance purchasing option?

- A. Reserved Instance
- B. Dedicated Instance
- C. On-Demand Instance
- D. **Spot Instance (correct)**

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **D. Spot Instance**.

The other response options are incorrect because:

- A. Reserved Instances require a contract length of either 1 year or 3 years. The workload in this scenario will only be running for 6 months.
- B. Dedicated Instances run in a virtual private cloud (VPC) on hardware that is dedicated to a single customer. They have a higher cost than the other response options, which run on shared hardware.
- C. On-Demand Instances fulfill the requirements of running for only 6 months and withstanding interruptions. However, a Spot Instance would be an ideal choice, because it does not require a minimum contract length, can withstand interruptions, and costs less than an On-Demand Instance.

Knowledge check question 4



85

A customer wants to give users messages for the specific topics to which they have subscribed. Which service should they use?

- A. Amazon Simple Notification Service (Amazon SNS)
- B. AWS Lambda
- C. Amazon Simple Queue Service (Amazon SQS)
- D. Amazon Elastic Kubernetes Service (Amazon EKS)

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

A customer wants to give users messages for the specific topics to which they have subscribed. Which service should they use?

- A. Amazon Simple Notification Service (Amazon SNS)
- B. AWS Lambda
- C. Amazon Simple Queue Service (Amazon SQS)
- D. Amazon Elastic Kubernetes Service (Amazon EKS)

Knowledge check answer 4



86

A customer wants to give users messages for the specific topics to which they have subscribed. Which service should they use?

- A. **Amazon Simple Notification Service (Amazon SNS) (correct)**
- B. AWS Lambda
- C. Amazon Simple Queue Service (Amazon SQS)
- D. Amazon Elastic Kubernetes Service (Amazon EKS)

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **A. Amazon Simple Notification Service (Amazon SNS)**.

The other response options are incorrect because:

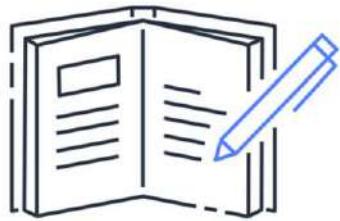
- B. AWS Lambda is a service that lets you run code without provisioning or managing servers.
- C. Amazon Simple Queue Service (Amazon SQS) is a service that allows you to send, store, and receive messages between software components through a queue. It does not use the message subscription and topic model that is involved with Amazon SNS.
- D. Amazon Elastic Kubernetes Service (Amazon EKS) is a fully managed Kubernetes service. Kubernetes is open-source software that allows you to deploy and manage containerized applications at scale.

Module 2 summary



In this module, you learned how to:

- Describe Amazon EC2 benefits
- Identify the Amazon EC2 instance types
- Differentiate among Amazon EC2 billing options
- Summarize Amazon EC2 Auto Scaling benefits
- Summarize Elastic Load Balancing benefits
- Provide examples of Elastic Load Balancing uses
- Describe differences between Amazon SNS and Amazon SQS
- Summarize additional AWS compute options



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

97

In this module, you learned how to:

- Describe Amazon EC2 benefits
- Identify the Amazon EC2 instance types
- Differentiate among Amazon EC2 billing options
- Summarize Amazon EC2 Auto Scaling benefits
- Summarize Elastic Load Balancing benefits
- Provide examples of Elastic Load Balancing uses
- Describe differences between Amazon SNS and Amazon SQS
- Summarize additional AWS compute options

The next module delves into the AWS global infrastructure.

Module 3

Global Infrastructure and Reliability



In this module, you will learn about the AWS Global Infrastructure and ways to interact with AWS services.

Module 3 objectives



In this module, you will learn how to:

- Summarize the AWS Global Infrastructure benefits
- Describe Availability Zones
- Describe the benefits of Amazon CloudFront and edge locations.
- Compare methods for provisioning AWS services.



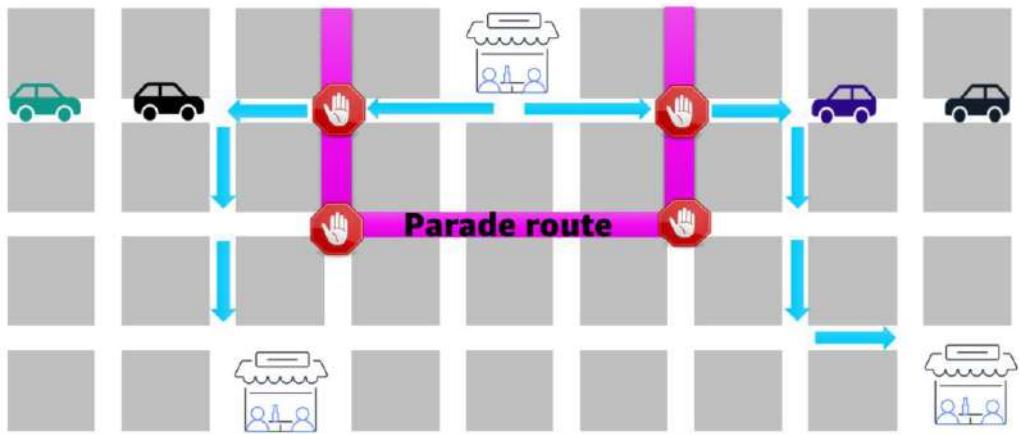
© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

89

In this module, you will learn how to:

- Summarize the benefits of the AWS Global Infrastructure
- Describe the basic concept of Availability Zones
- Describe the benefits of Amazon CloudFront and edge locations
- Compare different methods for provisioning AWS services

Build a global footprint



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

90

To understand the AWS Global Infrastructure, begin with an example from the coffee shop. Customers are unable to get to the coffee shop because a parade is blocking the road.

<click> If an event such as a parade, flood, or power outage impacts one location, customers can still get their coffee by visiting a different location only a few blocks away.

This is similar to how the AWS Global Infrastructure works.



Demo: Explore the AWS Global Infrastructure

<Note to Presenter: Do a quick demo of the AWS Global Infrastructure site (https://aws.amazon.com/about-aws/global-infrastructure/regions_az) to show students some of the Regions and around the world. Select a Region on the map and explain how it is composed of several Availability Zones.>

Around the world, AWS builds Regions closest to where the business traffic demands. Each Region contains multiple data centers that have all the components necessary to run your applications. Examples include compute, storage, networking, and security services.

Each Region connects to other Regions through fiber controlled by AWS. These connections enable your application components to run in separate Regions but still communicate with each other throughout the AWS Global Infrastructure.

When deploying applications on AWS, you choose which Region or Regions your applications will run in. You must consider four business factors when selecting a Region.

Select a Region



Determine the right Region for your services, data, and applications based on:



Compliance with data governance and legal requirements



Proximity to your customers



Available services within a Region



Pricing

When determining the right Region for your services, data, and applications, consider these four business factors:

- **Compliance with data governance and legal requirements** – Depending on your company and location, you might need to run your data out of specific areas. For example, if your company requires all of its data to reside within the boundaries of the UK, you would choose the London Region. Not all companies have location-specific data regulations, so you might need to focus more on the other three factors.
- **Proximity to your customers** – Selecting a Region that is close to your customers will help you to get content to them faster. For example, your company is based in Washington, DC, and many of your customers live in Singapore. You might consider running your infrastructure in the Northern Virginia Region to be close to company headquarters, and run your applications from the Singapore Region.
- **Available services within a Region** – Sometimes, the closest Region might not have all the features that you want to offer to customers. AWS is frequently

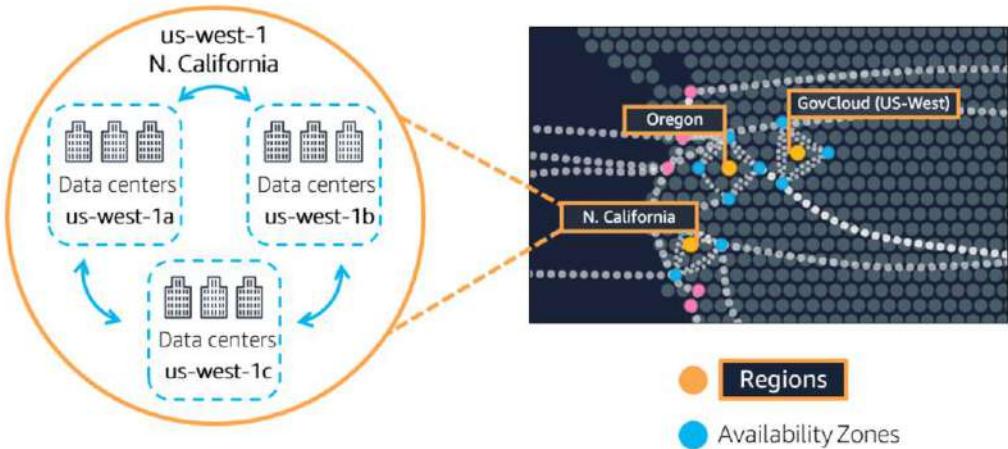
innovating by creating new services and expanding on features within existing services. However, making new services available around the world sometimes requires AWS to build out physical hardware one Region at a time. Suppose that your developers want to build an application that uses Amazon Braket (AWS quantum computing platform). As of this course, Amazon Braket is not yet available in every AWS Region around the world, so your developers would have to run it in one of the Regions that already offers it.

- **Pricing** – Suppose that you are considering running applications in both the United States and Brazil. The way Brazil's tax structure is set up, it might cost 50% more to run the same workload out of the São Paulo Region compared to the Oregon Region. You will learn in more detail that several factors determine pricing, but for now know that the cost of services can vary from Region to Region.

Spanning multiple Regions helps to keep your applications and data safe from disasters. However, this isn't the only way to get high availability and fault tolerance in the AWS Global Infrastructure. Regions are made up of multiple **Availability Zones**.

Availability Zones

aws training and certification



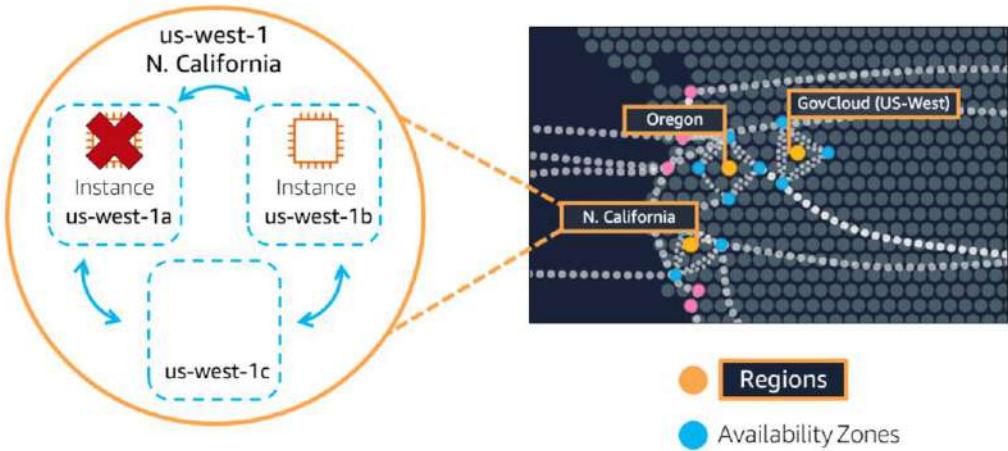
© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

95

An Availability Zone is a single data center or a group of data centers within a Region. If a disaster occurs in one part of the Region, the geographical distance helps to ensure that not all Availability Zones are affected. Availability Zones are located tens of miles apart from each other. This helps them to provide interconnectivity to support the services and applications that run within a Region.

Even though Availability Zones are close enough to have low latency (the time between when content is requested and received), they are not built directly next to one another.

Amazon EC2 instances in multiple AZs



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

94

Here's an example. Suppose that you're running an application on a single Amazon EC2 instance in the Northern California Region. The instance is running in the us-west-1a Availability Zone. If us-west-1a were to fail, you would lose your instance.

<click> A best practice is to run applications across at least two Availability Zones in a Region. In this example, you might choose to run a second Amazon EC2 instance in us-west-1b. If us-west-1a were to fail, your application would still be running in us-west-1b.

Discussion

What is the relationship between Regions and Availability Zones?

<Note to Presenter: For this discussion, ensure that learners have mentioned the following key points.>

Regions consist of two or more Availability Zones. Each Availability Zone includes one or more data centers.

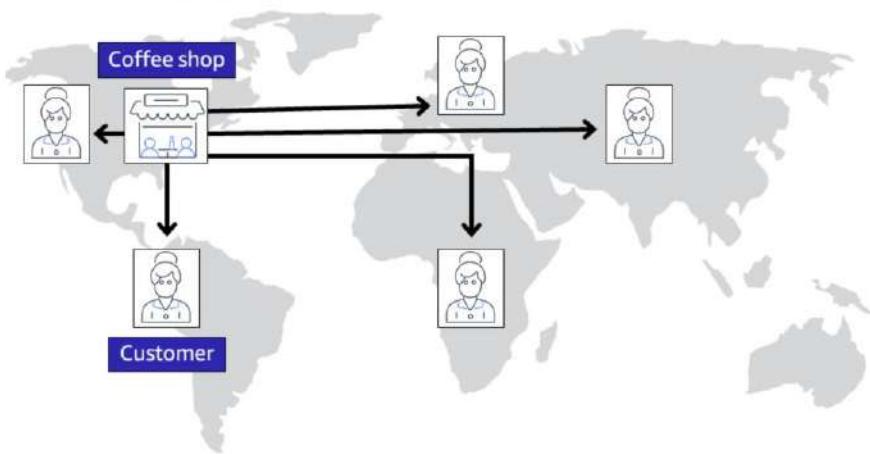
After you have selected a Region for your applications, as a best practice, run applications in multiple Availability Zones. This helps to ensure that your applications can continue to run if one Availability Zone fails.

Get closer to your customers

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



Global content delivery

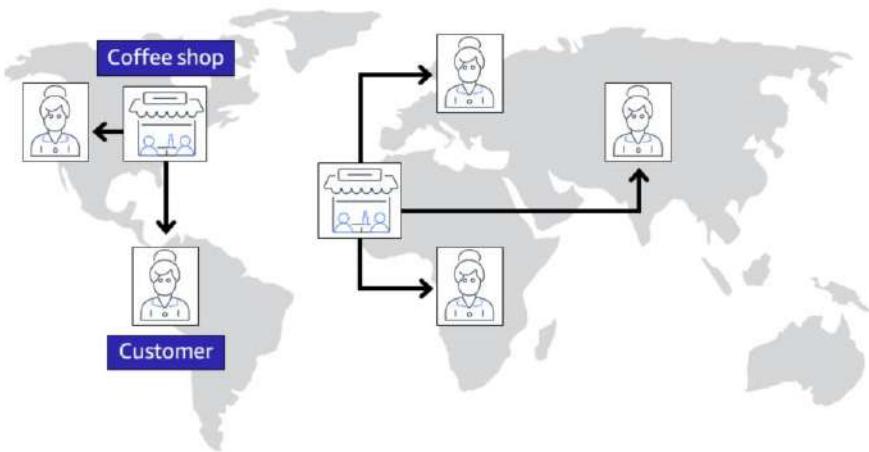


© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

97

Suppose that the coffee shop's online store has attracted customers from all over the world. The coffee shop ships its products worldwide. However, it can take a long time for these products to be delivered to customers who live far away from the shop.

Global content delivery



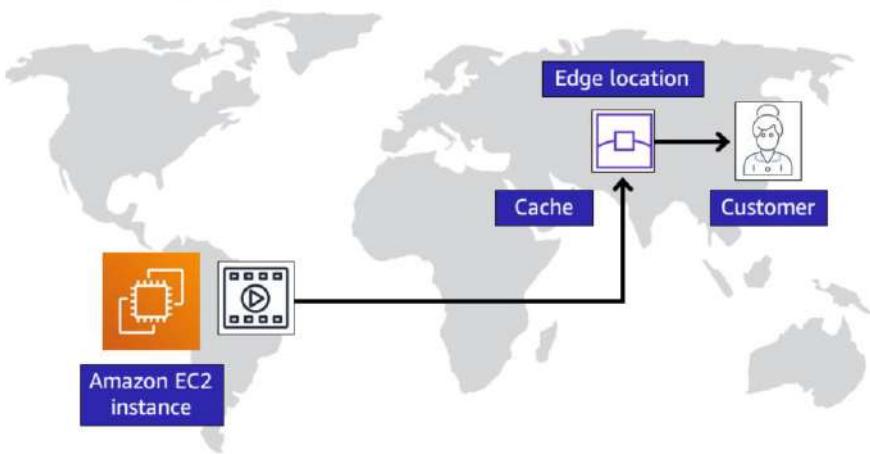
© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

91

To reduce the time it takes to deliver products to customers, the coffee shop opens a new location that is closer to customers in other parts of the world. Customers are able to receive the same products as before, but at quicker speeds because of their proximity to the new shop.

This is similar to how content is delivered throughout the AWS Global Infrastructure. Instead of shipping coffee beans to your customers, you might provide them with images, videos, webpages, and other types of electronic data.

Amazon CloudFront delivers content



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

99

Opening new stores is similar to using **edge locations** to bring content closer to your customers. An edge location is a site that Amazon CloudFront uses to store cached copies of your content for faster delivery to customers.

For example, suppose that your company's data is stored in Brazil, and you have customers who live in China. To provide content to these customers, you don't need to move all the content to one of the Chinese Regions. Instead of requiring your customers to get their data from Brazil, you can cache a copy locally at an edge location that is close to your customers in China.

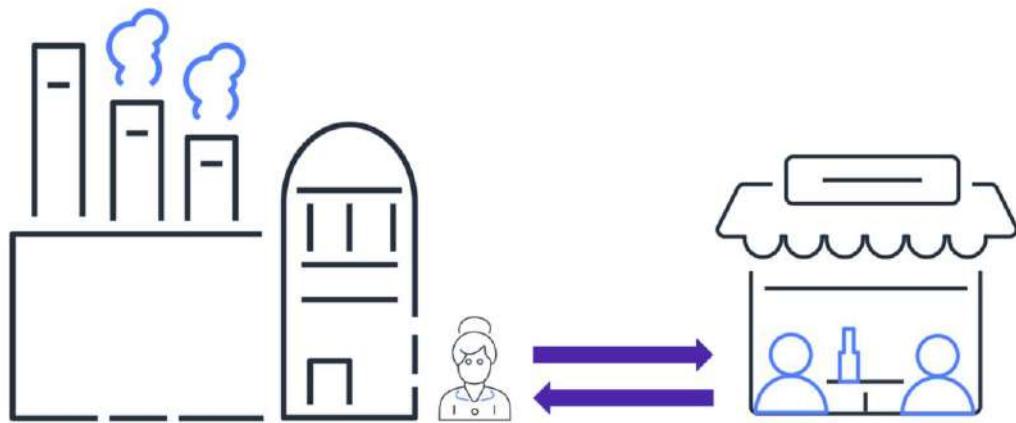
When a customer in China requests one of your files, Amazon CloudFront retrieves the file from the cache in the edge location and delivers the file to the customer. The file is delivered to the customer faster because it came from the edge location near China rather than from the original source in Brazil.

AWS Outposts

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



Get products from the coffee shop



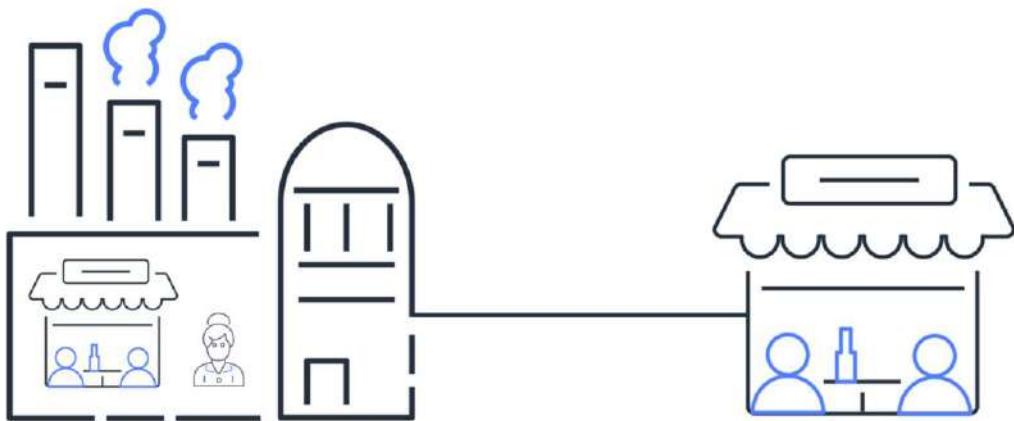
© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

101

Suppose that a company is located a few blocks away from the coffee shop. Employees from the company frequently visit the coffee shop and bring back their items to work.

However, the employees would prefer not to leave their building to get coffee. Leaving the building requires them to take time away from their data-intensive and time-sensitive workloads, such as real-time data processing, controlling onsite equipment, and so on.

Get products from the coffee shop



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

102

The company owners decide to open an operational coffee shop in their building. The main coffee shop now has a link to the new onsite shop within the company. Only the company's employees, who can now complete their work and get coffee without needing to leave their building, will use this new location.

The main coffee shop location remains open and operational. If the company's employees stop by the main coffee shop location on their way to work or on the way home, all of their personal information (such as their order history, rewards information, and so on) is accessible there. The personal information remains in sync with the onsite shop's records.

This is an example of the functionality that **AWS Outposts** provides.

AWS Outposts



AWS Outposts



Extend AWS infrastructure and services to your on-premises data center

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

103

AWS Outposts is a service that you can use to run AWS infrastructure, services, and tools within your own on-premises data center in a hybrid cloud approach.

AWS Outposts allows you to support workloads with data-intensive or time-sensitive requirements. Examples include the ones mentioned in the coffee shop scenario (real-time data processing and controlling onsite equipment). You can think of the products that the coffee shop provides as AWS resources, such as Amazon EC2 instances, AWS Lambda functions, and so on.

When an Outpost installs at your on-premises location, it connects to the nearest AWS Region. You continue to access, monitor, and manage your AWS services just as you would if your applications were running in the cloud.

Whether AWS Outposts meets your company's needs for a hybrid cloud deployment, consider your company's network connectivity. To access your AWS services and resources, your on-premises location must maintain ongoing connectivity to the nearest AWS Region. AWS Outposts are not designed for environments with limited to no connectivity.

Discussion



When choosing an AWS Region for your services, data, and applications, why should you consider a Region's proximity to your customers?

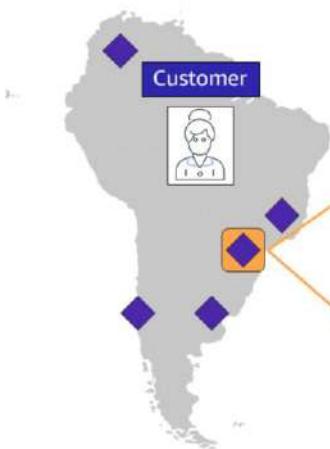
© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

So far, in this module, you have explored several aspects of the AWS Global Infrastructure: Regions, Availability Zones, and edge locations. Now, you will work through a scenario to put these pieces together.

In this scenario, you are a business leader who is researching options for how to deliver content to your customers.

Discussion question: When choosing an AWS Region for your services, data, and applications, why should you consider a Region's proximity to your customers?

Review: AWS Global Infrastructure



Region:
• São Paulo

Availability Zones:
• sa-east-1a
• sa-east-1b
• sa-east-1c

Edge locations

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

105

Choosing a Region that is close to your customers helps deliver content to them faster.

In this scenario, suppose that you are deploying an application used by your customers in Brazil.

<click> First, you choose to deploy your application in the São Paulo Region (sa-east-1) because this is the closest Region to your customers in Brazil.

<click> The São Paulo Region includes three Availability Zones: sa-east-1a, sa-east-1b, and sa-east-1c.

Discussion question: Why is it a best practice to deploy applications and resources in more than one Availability Zone?

Suppose that your application is being supported by one Availability Zone, sa-east-1a. If sa-east-1a went down, your customers wouldn't be able to access your application. Now, suppose that two Availability Zones are supporting your application: sa-east-1a and sa-east-1b. In this case, if sa-east-1a went down, your application would remain

operational because sa-east-1b was unaffected.

<click> Finally, you can use Amazon CloudFront to store cached copies of your content at edge locations that are close to your customers. When your customers request content, it travels across a short distance and is delivered to them quickly.

Interact with AWS services

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



Perform actions through API requests



Order a cup of coffee.

Ask for a refill.

Check your rewards balance.



Launch an Amazon EC2 instance.

Create a load balancer.

Invoke an AWS Lambda function.

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

107

Take a moment to think about some of the actions that you might perform when you are in a coffee shop. Some of these actions might include:

- Order a cup of coffee.
- Ask for a refill.
- Check your rewards balance, and so on.

In AWS, some of the actions that you could take to interact with services might include:

- Launch an Amazon EC2 instance.
- Create a load balancer.
- Invoke an AWS Lambda function, and so on.

These AWS actions are examples of **application programming interface (API) requests**. API requests are predetermined ways for you to interact with AWS services. You can use API requests to provision, manage, and configure your AWS resources.

You can access and interact with AWS services in three ways: the AWS Management Console, the AWS Command Line Interface (AWS CLI), and software development kits (SDKs).

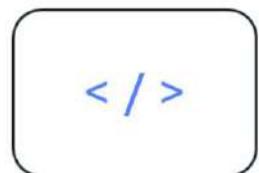
Interact with AWS services



AWS Management Console



AWS Command Line Interface (AWS CLI)



Software development kits (SDKs)

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

108

The **AWS Management Console** is a web-based interface for accessing and managing AWS services. You can quickly access recently used services and search for other services by name, keyword, or acronym. The console includes wizards and automated workflows that can simplify the process of completing tasks.

You can also use the AWS Management Console mobile application to perform tasks such as monitoring resources, viewing alarms, and accessing billing information. Multiple identities can stay logged into the AWS Management Console mobile app at the same time.

Next, to save time when making API requests, you can use the **AWS Command Line Interface (AWS CLI)**. AWS CLI helps you control multiple AWS services directly from the command line within one tool. AWS CLI is available for users on Windows, macOS, and Linux.

By using AWS CLI, you can automate the actions that your services and applications perform through scripts. For example, you can use commands to launch an Amazon EC2 instance, connect an Amazon EC2 instance to a specific Auto Scaling group, and more.

Another option for accessing and managing AWS services is the **software development kits (SDKs)**. SDKs make it easier for you to use AWS services through an API designed for your programming language or platform. SDKs helps you use AWS services with your existing applications or create entirely new applications that will run on AWS.

To help you get started with using SDKs, AWS provides documentation and sample code for each supported programming language. Supported programming languages include C++, Java, .NET, and more.



Demo: AWS Management Console

Note to Presenter: *The demo is a high-level overview of how to navigate through the AWS Management Console, including:*

- ***Opening the list of all services***
- ***Accessing recently visited services***
- ***Finding a service by name, keyword, or acronym***
- ***Browsing through the “Build a solution” and “Learn to build” sections at the bottom of the AWS Management Console home page***
- ***Creating service shortcuts in the Console toolbar***

Make sure to focus on services that have been covered up to this point in the course, such as Amazon EC2, AWS Lambda, Elastic Load Balancing, and so on.

Module 3

Knowledge check

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



Knowledge check question 1



111

Which of the following is TRUE for the AWS Global Infrastructure?

- A. An Availability Zone consists of a single Region.
- B. An Availability Zone consists of two or more Regions.
- C. A Region consists of a single Availability Zone.
- D. A Region consists of two or more Availability Zones.

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which of the following statements is TRUE for the AWS Global Infrastructure?

- A. An Availability Zone consists of a single Region.
- B. An Availability Zone consists of two or more Regions.
- C. A Region consists of a single Availability Zone.
- D. A Region consists of two or more Availability Zones.

Knowledge check answer 1



112

Which of the following is TRUE for the AWS Global Infrastructure?

- A. An Availability Zone consists of a single Region.
- B. An Availability Zone consists of two or more Regions.
- C. A Region consists of a single Availability Zone.
- D. **A Region consists of two or more Availability Zones. (correct)**

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **D. A Region consists of two or more Availability Zones.**

For example, the South America (São Paulo) Region is sa-east-1. It includes three Availability Zones: sa-east-1a, sa-east-1b, and sa-east-1c.

Knowledge check question 2



115

Which factors should be considered when selecting a Region? (Select TWO.)

- A. Compliance with data governance and legal requirements
- B. Proximity to your customers
- C. Access to 24/7 technical support
- D. Ability to assign custom permissions to different users
- E. Access to the AWS Command Line Interface (AWS CLI)

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which factors should be considered when selecting a Region? (Select TWO.)

- A. Compliance with data governance and legal requirements
- B. Proximity to your customers
- C. Access to 24/7 technical support
- D. Ability to assign custom permissions to different users
- E. Access to the AWS Command Line Interface (AWS CLI)

Knowledge check answer 2



114

Which factors should be considered when selecting a Region? (Select TWO.)

- A. **Compliance with data governance and legal requirements (correct)**
- B. **Proximity to your customers (correct)**
- C. Access to 24/7 technical support
- D. Ability to assign custom permissions to different users
- E. Access to the AWS Command Line Interface (AWS CLI)

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct two response options are:

- A. Compliance with data governance and legal requirements**
- B. Proximity to your customers**

Two other factors to consider when selecting a Region are pricing and the services that are available in a Region.

The other response options are incorrect because:

- C. The level of support that you choose is not determined by Region. AWS Support plans are explored later in this course.
- D. Assigning custom permissions to different users is a feature that is possible in all AWS Regions.
- E. The AWS Command Line Interface (AWS CLI) is available in all AWS Regions.

Knowledge check question 3



115

Which statement best describes Amazon CloudFront?

- A. A service that allows you to run infrastructure in a hybrid cloud approach
- B. A serverless compute engine for containers
- C. A service that allows you to send and receive messages between software components through a queue
- D. A global content delivery service

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which statement best describes Amazon CloudFront?

- A. A service that allows you to run infrastructure in a hybrid cloud approach
- B. A serverless compute engine for containers
- C. A service that allows you to send and receive messages between software components through a queue
- D. A global content delivery service

Knowledge check answer 3



116.

Which statement best describes Amazon CloudFront?

- A. A service that allows you to run infrastructure in a hybrid cloud approach
- B. A serverless compute engine for containers
- C. A service that allows you to send and receive messages between software components through a queue
- D. **A global content delivery service (correct)**

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **D: A global content delivery service.**

Amazon CloudFront is a content delivery service. It uses a network of edge locations to cache content and deliver content to customers all over the world. When content is cached, it is stored locally as a copy. This content might be video files, photos, webpages, and so on.

The other response options are incorrect because:

- A. *AWS Outposts* is a service that allows you to run infrastructure in a hybrid cloud approach.
- B. *AWS Fargate* is a serverless compute engine for containers.
- C. *Amazon Simple Queue Service (Amazon SQS)* is a service that allows you to send, store, and receive messages between software components through a queue.

Knowledge check question 4



117

Which site does Amazon CloudFront use to cache copies of content for faster delivery to users at any location?

- A. Edge location
- B. Region
- C. Availability Zone
- D. Origin

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which site does Amazon CloudFront use to cache copies of content for faster delivery to users at any location?

- A. Edge location
- B. Region
- C. Availability Zone
- D. Origin

Knowledge check answer 4



118.

Which site does Amazon CloudFront use to cache copies of content for faster delivery to users at any location?

- A. Edge location (correct)
- B. Region
- C. Availability Zone
- D. Origin

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **A. Edge location**.

The other response options are incorrect because:

- B. A Region is a separate geographical location with multiple locations that are isolated from each other.
- C. An Availability Zone is a fully isolated portion of the AWS Global Infrastructure.
- D. An origin is the server from which CloudFront gets your files. Examples of CloudFront origins include Amazon Simple Storage Service (Amazon S3) buckets and web servers. (**Note:** Amazon S3 is explored later in this course.)

Knowledge check question 5



119

Which actions can you perform with AWS Outposts?

- A. Automate actions for AWS services and applications through scripts
- B. Access wizards and automated workflows to perform tasks in AWS services
- C. Extend AWS infrastructure and services to your on-premises data center
- D. Develop AWS applications in supported programming languages

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which actions can you perform with AWS Outposts?

- A. Automate actions for AWS services and applications through scripts
- B. Access wizards and automated workflows to perform tasks in AWS services
- C. Extend AWS infrastructure and services to your on-premises data center
- D. Develop AWS applications in supported programming languages

Knowledge check answer 5



120

Which actions can you perform with AWS Outposts?

- A. Automate actions for AWS services and applications through scripts
- B. Access wizards and automated workflows to perform tasks in AWS services
- C. Extend AWS infrastructure and services to your on-premises data center (correct)
- D. Develop AWS applications in supported programming languages

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **C: Extend AWS infrastructure and services to your on-premises data center.**

The other response options are incorrect because:

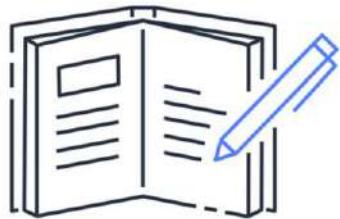
- A. The AWS Command Line Interface (AWS CLI) is used to automate actions for AWS services and applications through scripts.
- B. The AWS Management Console includes wizards and workflows that you can use to complete tasks in AWS services.
- D. Software development kits (SDKs) allow you to develop AWS applications in supported programming languages.

Module 3 summary



In this module, you learned about:

- Three aspects of the AWS Global Infrastructure
- Four factors to consider when selecting an AWS Region
- Three ways to interact with AWS services



In this module, you examined three aspects of the AWS Global Infrastructure:

- Regions
- Availability Zones
- Amazon CloudFront edge locations

You also explored four factors that you should consider when selecting a Region for your AWS applications and resources:

- Compliance with data governance and legal requirements
- Proximity to your customers
- Available services within a Region
- Pricing

Finally, you learned about the three ways to interact with AWS services:

- AWS Management Console
- AWS Command Line Interface (AWS CLI)
- Software development kits (SDKs)

The next module explores some of the networking services that AWS offers.

Module 4

Networking



In this module, you will learn about Amazon Virtual Private Cloud (Amazon VPC), network access control lists (ACLs), security groups, and Amazon Route 53.

Module 4 objectives



In this module, you will learn how to:

- Describe basic networking concepts
- Describe the differences between public and private networking resources
- Explain a virtual private gateway using a real-life scenario
- Explain a VPN using a real-life scenario
- Describe AWS Direct Connect benefits
- Describe hybrid deployment benefits
- Describe the layers of security in an IT strategy
- Describe the services customers use to interact with the AWS global network



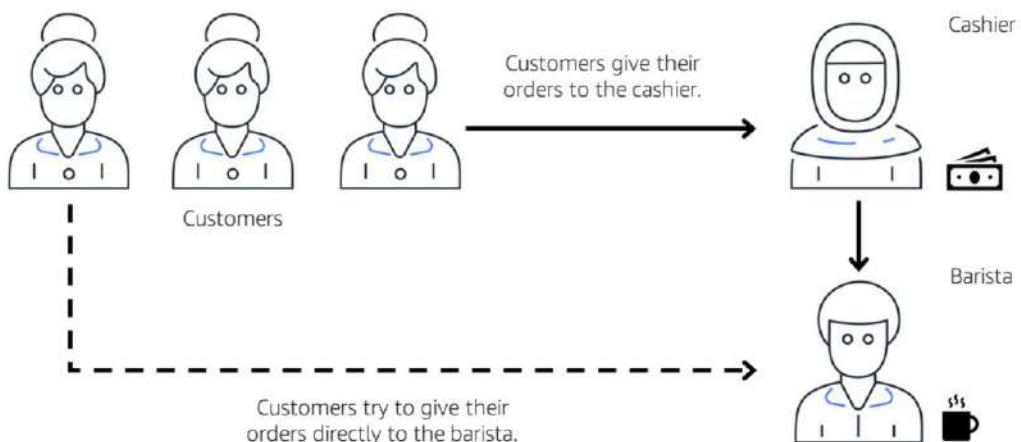
© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

123

In this module, you will learn how to:

- Describe the basic concepts of networking
- Describe the differences between public and private networking resources
- Explain a virtual private gateway using a real life scenario
- Explain a virtual private network (VPN) using a real life scenario
- Describe AWS Direct Connect benefits
- Describe hybrid deployment benefits
- Describe the layers of security in an IT strategy
- Describe the services customers use to interact with the AWS global network

Traffic in the coffee shop



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

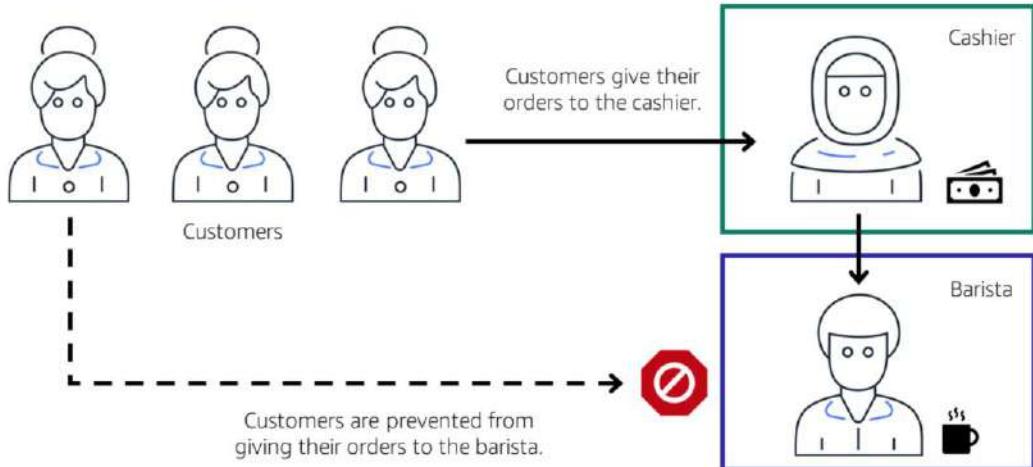
124

This section explores AWS networking services, beginning with an example from the coffee shop.

First, customers give their orders to the cashier. The cashier then passes the orders to the barista. This process allows the line to keep running smoothly as more customers come in.

<click> Suppose that some customers try to skip the cashier line and give their orders directly to the barista. This disrupts the flow of traffic and results in customers accessing a part of the coffee shop that is off limits to them.

Traffic in the coffee shop



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

125

To fix this, the owners of the coffee shop divide the counter area by placing the cashier and the barista in separate workstations. The cashier's workstation is public facing and designed to receive customers. The barista's area is private. The barista can still receive orders from the cashier but not directly from customers.

This is similar to how you can use AWS networking services to isolate resources and determine exactly how network traffic flows.

Imagine the millions of customers who use AWS services. Also, imagine the millions of resources that these customers have created, such as Amazon EC2 instances. Without boundaries around all of these resources, network traffic would be able to flow between them, unrestricted.

A networking service that you can use to establish boundaries around your AWS resources is **Amazon Virtual Private Cloud (Amazon VPC)**.

Amazon Virtual Private Cloud (Amazon VPC)

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.





Amazon Virtual Private Cloud (Amazon VPC) enables you to launch resources in a virtual network that you define.



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

127

Amazon VPC enables you to provision an isolated section of the AWS Cloud. In this isolated section, you can launch resources in a virtual network that you define. Within a virtual private cloud (VPC), you can organize your resources into subnets.

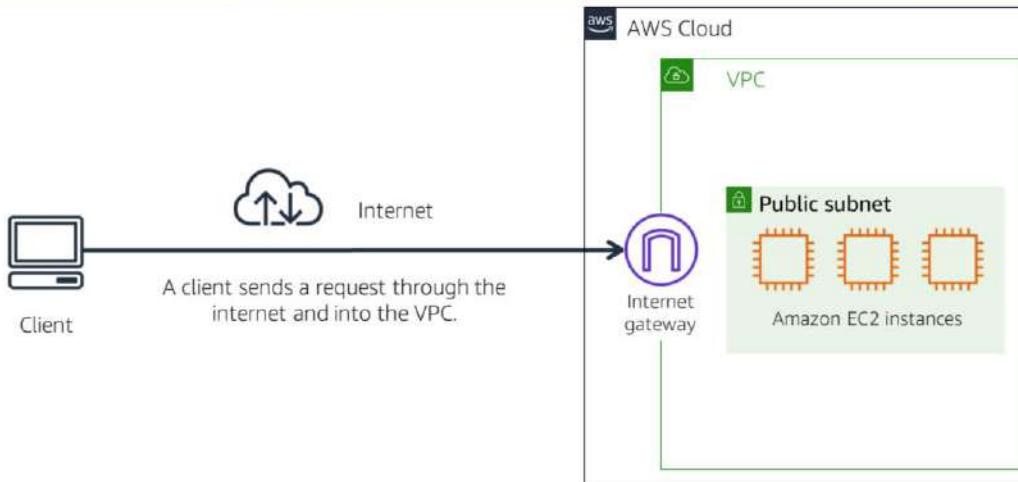
A **subnet** is a section of a VPC that can contain resources such as Amazon EC2 instances.

<click> In the coffee shop, you can think of the counter area as a VPC. The counter area divides into two separate areas for the cashier's workstation and the barista's workstation.

Next, you will see how to access public resources within a VPC.

Internet gateway

aws training and certification



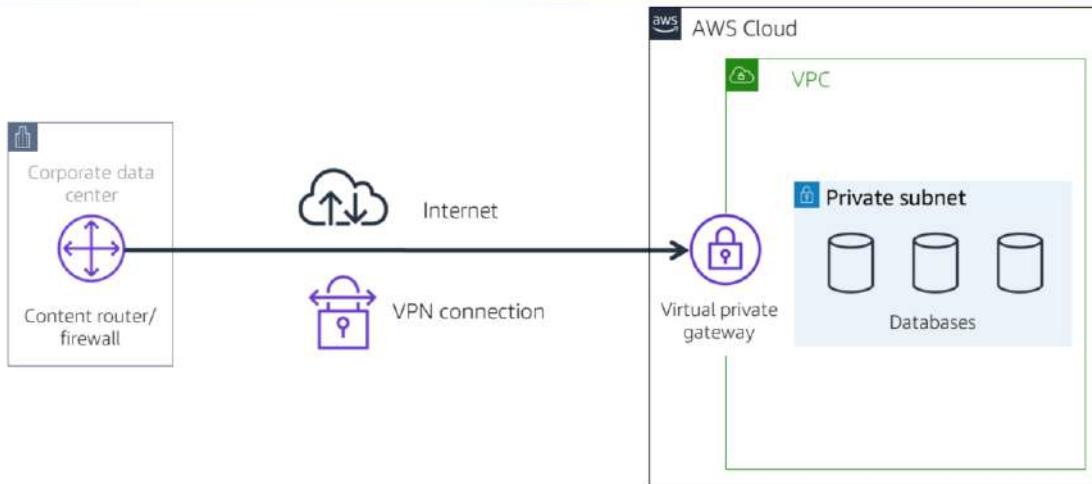
© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

128

To allow public traffic from the internet to access your VPC, you attach an **internet gateway** to the VPC.

An internet gateway is a connection between a VPC and the internet. You can think of an internet gateway as being similar to a doorway that customers use to enter the coffee shop. Without an internet gateway, no one can access the resources within your VPC.

Virtual private gateway



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

129

Next, to access private resources in a VPC, you can use a **virtual private gateway**.

Here's an example of how a virtual private gateway works. You can think of the internet as the road between your home and the coffee shop. Suppose that you are traveling on this road with a bodyguard to protect you. You are still using the same road as other customers, but with an extra layer of protection.

<click> The bodyguard is like a VPN connection that encrypts (or protects) your internet traffic from all the other requests around it.

<click> The virtual private gateway is the component that allows protected internet traffic to enter into the VPC.

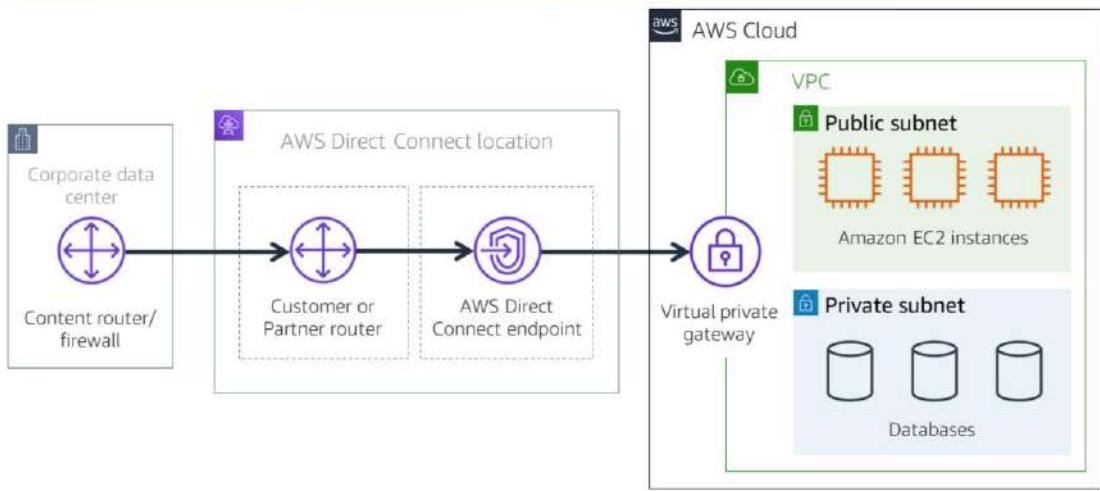
Even though your connection to the coffee shop has extra protection, traffic jams are possible because you're using the same road as other customers.

A virtual private gateway enables you to establish a virtual private network (VPN) connection between your VPC and a private network, such as an on-premises data center or internal corporate network. A virtual private gateway allows traffic into the

VPC only if it is coming from an approved network.

Another option that you can use to get from your private network to the VPC is AWS Direct Connect.

AWS Direct Connect



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

150

AWS Direct Connect is a service that enables you to establish a dedicated private connection between your data center and VPC.

Suppose that there is an apartment building with a hallway directly linking the building to the coffee shop. Only the residents of the apartment building are allowed to travel through this hallway.

<click> This private hallway provides the same type of dedicated connection as AWS Direct Connect. Residents are able to get into the coffee shop without needing to use the public road that is shared with other customers.

The private connection that AWS Direct Connect provides helps you to reduce network costs and increase the amount of bandwidth that can travel through your network.

Subnets



A **subnet** is a section in a VPC in which you can place groups of isolated resources.

A subnet can be public or private.



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

151

A **subnet** is a section in a VPC in which you can group resources based on security or operational needs. Subnets can be public or private.

- *Public subnets* contain resources that need to be accessible by the public, such as an online store's website.
- *Private subnets* contain resources that should be accessible only through your private network, such as a database that contains customers' personal information and order histories.

Within a VPC, subnets can communicate with each other. For example, you might have an application that involves Amazon EC2 instances in a public subnet communicating with databases that are located in a private subnet.

Match: VPC components



1. Isolate databases containing customers' personal information
2. Create a VPN connection between the VPC and the internal corporate network
3. Support a customer-facing website
4. Establish a dedicated connection between an on-premises data center and the VPC

- A. Public subnet
- B. Private subnet
- C. Virtual private gateway
- D. AWS Direct Connect

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

152

For this review exercise, imagine that your company is launching an online photo storage application. Help determine which VPC component should be used for certain aspects of the application.

When customers create an account in the application, they must provide personal information such as their email address and date of birth. Which VPC component should you use to isolate the databases that contain customers' personal information?

Match: VPC components



1. Isolate databases containing customers' personal information

A. Public subnet

2. Create a VPN connection between the VPC and the internal corporate network

B. Private subnet

3. Support a customer-facing website

C. Virtual private gateway

4. Establish a dedicated connection between an on-premises data center and the VPC

D. AWS Direct Connect

Use a **private subnet** to isolate databases containing customers' personal information. Private subnets contain resources that should be accessible only through your private network.

Your company has an internal corporate network that needs to communicate with the VPC. Which component should you use to create a VPN connection between the VPC and the internal corporate network?

Match: VPC components



1. Isolate databases containing customers' personal information

A. Public subnet

2. Create a VPN connection between the VPC and the internal corporate network

B. Private subnet

3. Support a customer-facing website

C. Virtual private gateway

4. Establish a dedicated connection between an on-premises data center and the VPC

D. AWS Direct Connect

Use a **virtual private gateway** to create a VPN connection between the VPC and your company's internal network.

The photos that customers upload to the website must be accessible by anyone on the internet. You are storing the photo files in Amazon Simple Storage Service (Amazon S3) buckets. (**Note:** Amazon S3 is explored in the next module.)

Which VPC component should you use to support the customer-facing website?

Match: VPC components



1. Isolate databases containing customers' personal information
2. Create a VPN connection between the VPC and the internal corporate network
3. Support a customer-facing website
4. Establish a dedicated connection between an on-premises data center and the VPC

A. Public subnet

B. Private subnet

C. Virtual private gateway

D. AWS Direct Connect

Use a **public subnet** to support the customer-facing website. Public subnets contain resources that must be accessible by the public.

The online photo storage application will use substantial bandwidth, so your company wants to create a dedicated connection to the VPC. Which option should you use to establish a dedicated connection between your on-premises data center and the VPC?

Match: VPC components



1. Isolate databases containing customers' personal information

A. Public subnet

2. Create a VPN connection between the VPC and the internal corporate network

B. Private subnet

3. Support a customer-facing website

C. Virtual private gateway

4. Establish a dedicated connection between an on-premises data center and the VPC

D. AWS Direct Connect

Use **AWS Direct Connect** to establish a dedicated connection between your on-premises data center and the VPC.

Network access control lists and security groups

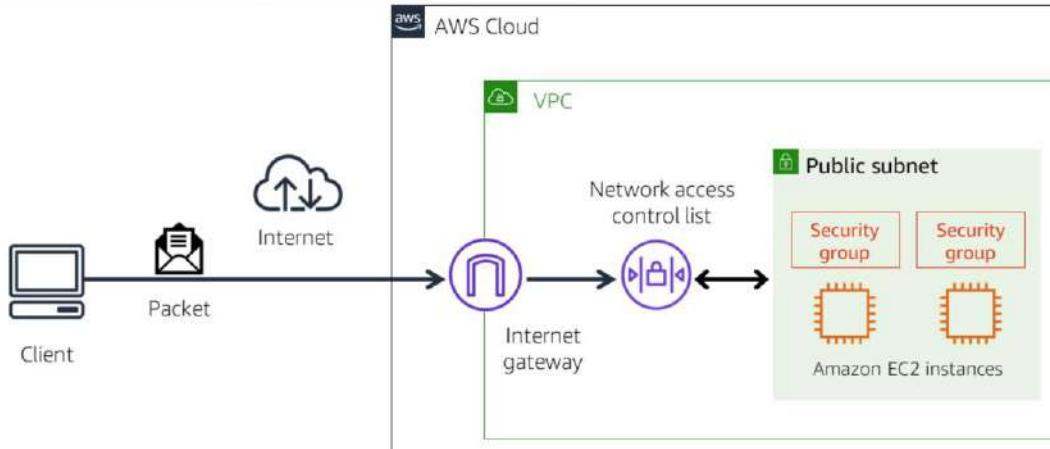
© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



So far, in this module, you have learned about methods for securing the entire perimeter around a VPC.

This section describes two additional features for securing the resources within a VPC: network access control lists (ACLs) and security groups.

Network traffic in a VPC



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

158

This section explores how resources in a VPC can communicate through the internet.

<click> When a customer requests data from an application that is hosted in the AWS Cloud, this request is sent as a **packet**. A packet is a unit of data sent over the internet or a network.

<click> It enters into a VPC through an internet gateway. Before a packet can enter into a subnet or exit from a subnet, it checks for permissions. These permissions indicate who sent the packet and how the packet is trying to communicate with the resources within a subnet.

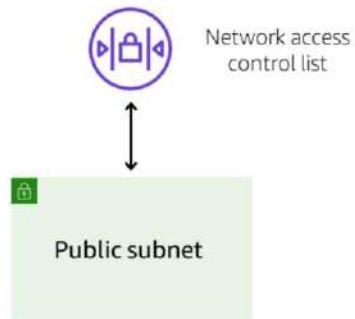
<click> The VPC component that checks packet permissions for subnets is a **network access control list (ACL)**.

Network access control lists



A **network access control list (network ACL)** is a virtual firewall for a subnet. By default:

- The default network ACL allows all inbound and outbound traffic.
- Custom network ACLs deny all inbound and outbound traffic.



A **network access control list (ACL)** is a virtual firewall that controls inbound and outbound traffic at the subnet level.

For this example, step outside of the coffee shop and imagine that you are in an airport. In the airport, travelers are trying to enter into a different country. You can think of the travelers as packets and the passport control officer as a network ACL. The passport control officer checks travelers' credentials when they are both entering and exiting out of the country. If a traveler is on an approved list, they are able to get through. However, if they are not on the approved list or are explicitly on a list of banned travelers, they cannot come in.

Each AWS account includes a default network ACL. When configuring your VPC, you can use your account's default network ACL or create custom network ACLs.

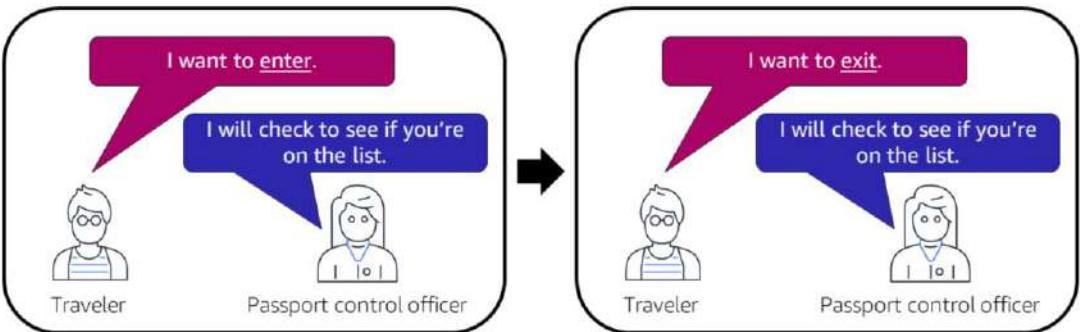
By default, your account's default network ACL allows all inbound and outbound traffic, but you can modify it by adding your own rules. For custom network ACLs, all inbound and outbound traffic is denied until you add rules to specify which traffic should be allowed. Additionally, all network ACLs have an explicit deny rule. This rule ensures that if a packet doesn't match any of the other rules on the list, the packet is

denied.

Stateless packet filtering



- Network ACLs perform **stateless** packet filtering.
- Before a packet can exit a subnet, it must be checked against the outbound rules.



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

140

Network ACLs perform **stateless** packet filtering. They remember nothing and check packets that cross the subnet border each way: both inbound and outbound.

Recall the previous example of a traveler who wants to enter into a different country. This is similar to sending a request out from an Amazon EC2 instance and to the internet.

<click> When a packet response for that request comes back to the subnet, the network ACL does not remember your previous request. The network ACL checks the packet response against its list of rules to determine whether it is allowed or denied.

After a packet has entered a subnet, it must have its permissions evaluated for resources within the subnet, such as Amazon EC2 instances. The VPC component that checks packet permissions for an Amazon EC2 instance is a **security group**.

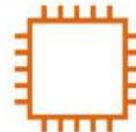
Security groups



A **security group** is a virtual firewall for an Amazon EC2 instance.

By default, a security group denies all inbound traffic and allows all outbound traffic.

Security group



Amazon EC2 instance

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

141

A **security group** is a virtual firewall that controls inbound and outbound traffic for an Amazon EC2 instance.

By default, a security group denies all inbound traffic and allows all outbound traffic. You can add custom rules to configure which traffic should be allowed or denied.

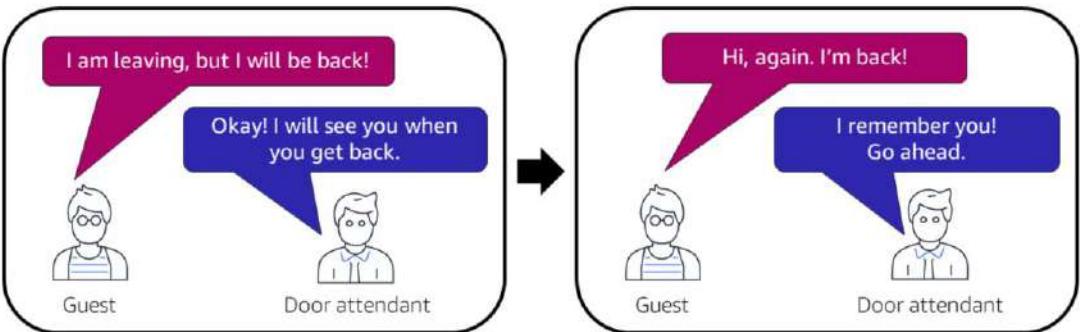
For this example, suppose that you are in an apartment building with a door attendant who greets guests in the lobby. You can think of the guests as packets and the door attendant as a security group. As guests arrive, the door attendant checks a list to ensure they can enter the building. However, the door attendant does not check the list again when guests are exiting the building.

If you have multiple Amazon EC2 instances within a subnet, you can associate them with the same security group or use different security groups for each instance.

Stateful packet filtering



- Security groups perform **stateful** packet filtering.
- They remember previous decisions that were made for incoming packets.



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

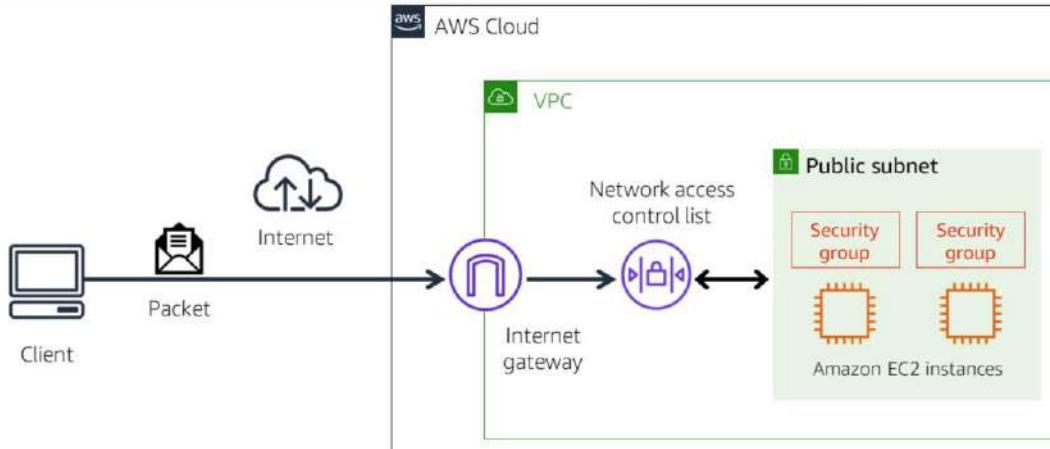
142

Security groups perform **stateful** packet filtering. They remember previous decisions that were made for incoming packets.

Consider the same example of sending a request out from an Amazon EC2 instance to the internet.

<click> When a packet response for that request comes back to the instance, the security group remembers your previous request and allows the response to proceed, regardless of inbound security group rules.

Network traffic in a VPC



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

143

You learned how packets travel into a virtual private cloud (VPC). A packet is a request from the internet. Packets come into a VPC through an internet gateway. Before a packet can enter into a subnet, it is evaluated against rules in a network ACL. Then if the packet wants to access an Amazon EC2 instance, its permissions are evaluated by a security group.

Both network ACLs and security groups enable you to configure custom rules for the traffic in your VPC. As you continue to learn more about AWS security and networking, make sure to understand the differences between network ACLs and security groups.

Knowledge check



144

What are the differences between network access control lists and security groups?

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

What are the differences between network access control lists and security groups?

Knowledge check



145

- Network access control lists are virtual firewalls for subnets. They perform stateless packet filtering.
- Security groups are virtual firewalls for Amazon EC2 instances. They perform stateful packet filtering.

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Network access control lists (ACLs) evaluate network traffic at the subnet level. They are stateless. ACLs do not remember previous traffic patterns or flows when evaluating packet permissions.

Security groups evaluate network traffic at the instance level. They are stateful. Security groups remember previous decisions that were made for incoming packets.

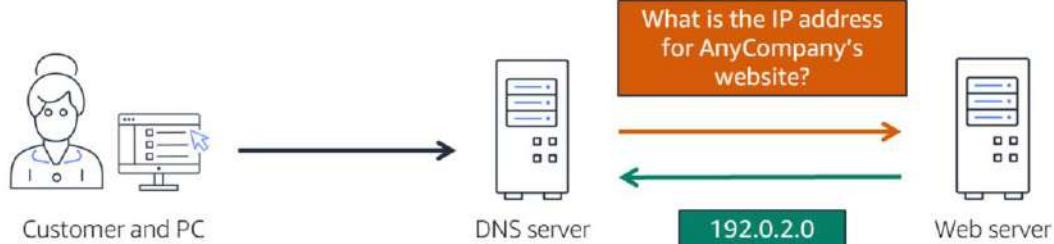
Interact with the AWS global network

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



Throughout this module, you have learned how you can interact with AWS by designing and deploying applications. Now you will examine how your customers can interact with AWS by accessing your applications.

Domain Name System (DNS)



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

147

Suppose that AnyCompany has a website hosted in the AWS Cloud. Customers enter the web address into their browser, and they are able to access the website. This happens because of **Domain Name System (DNS)** resolution. DNS resolution involves a DNS server communicating with a web server.

You can think of DNS as being the phone book of the internet. DNS resolution is the process of translating a domain name to an IP address.

<click> For example, suppose that you want to visit AnyCompany's website. When you enter the domain name into your browser, this request is sent to a DNS server.

<click> The DNS server asks the web server for the IP address that corresponds to AnyCompany's website.

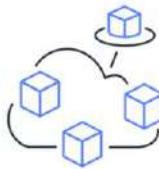
<click> The web server responds by providing the IP address for AnyCompany's website, 192.0.2.0.

Amazon Route 53 is the AWS service that provides DNS capabilities.

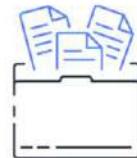
Amazon Route 53



Route users to internet applications



Connect user requests to infrastructure in AWS and outside of AWS



Manage DNS records for domain names

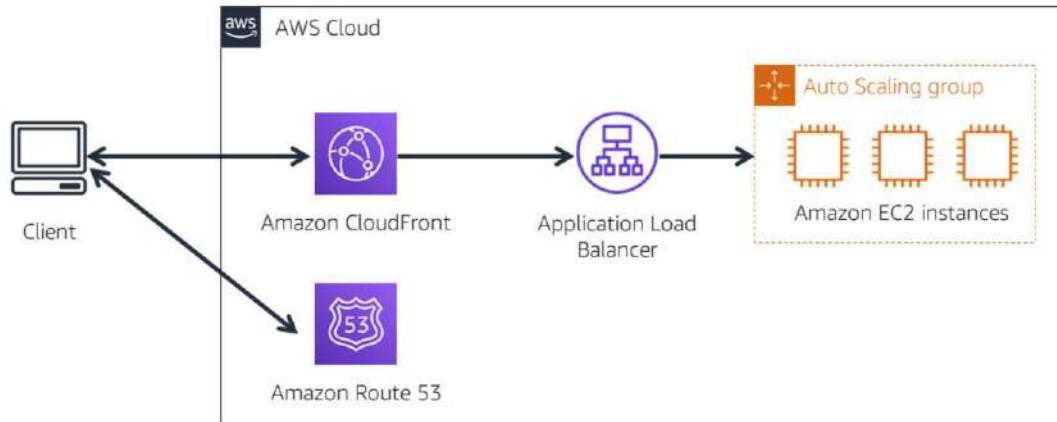
Amazon Route 53 is a DNS web service. It gives developers and businesses a reliable way to route end users to internet applications hosted in AWS.

Amazon Route 53 connects user requests to infrastructure running in AWS (such as Amazon EC2 instances and load balancers). It can route users to infrastructure outside of AWS.

Another feature of Route 53 is the ability to manage the DNS records for domain names. You can register new domain names directly in Route 53. You can also transfer DNS records for existing domain names managed by other domain registrars. This enables you to manage all of your domain names within a single location.

In the previous module, you learned about Amazon CloudFront, a content delivery service. The following example describes how Route 53 and Amazon CloudFront work together to deliver content to customers.

Amazon Route 53 and CloudFront



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

149

Suppose that AnyCompany's application is running on several Amazon EC2 instances. These instances are in an Auto Scaling group that attaches to an Application Load Balancer.

- A customer requests data from the application by going to AnyCompany's website.
- Amazon Route 53 uses DNS resolution to identify the AnyCompany website corresponding IP address, 192.0.2.0. This information is sent back to the customer.
- The customer's request routes to the nearest edge location through Amazon CloudFront.
- Amazon CloudFront connects to the Application Load Balancer, which sends the incoming packet to an Amazon EC2 instance.

Module 4

Knowledge check

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



Knowledge check question 1



151

Which component can be used to establish a private dedicated connection between a company's data center and AWS?

- A. Private subnet
- B. DNS
- C. AWS Direct Connect
- D. Virtual private gateway

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which component can be used to establish a private dedicated connection between a company's data center and AWS?

- A. Private subnet
- B. DNS
- C. AWS Direct Connect
- D. Virtual private gateway

Knowledge check answer 1



152

Which component can be used to establish a private dedicated connection between a company's data center and AWS?

- A. Private subnet
- B. DNS
- C. **AWS Direct Connect (correct)**
- D. Virtual private gateway

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **C. AWS Direct Connect**.

The other response options are incorrect because:

- A. A private subnet is a section of a VPC in which you can group resources that should be accessed only through your private network. Although it is private, it is not used for establishing a connection between a data center and AWS.
- B. DNS stands for Domain Name System, which is a directory used for matching domain names to IP addresses.
- C. A virtual private gateway enables you to create a VPN connection between your VPC and a private network, such as your company's data center. Although this connection is private and encrypted, it travels through the public internet, not through a dedicated connection.

Knowledge check question 2



155

Which statement describes security groups?

- A. They are stateful and allow all inbound traffic by default.
- B. They are stateful and deny all inbound traffic by default.
- C. They are stateless and allow all inbound traffic by default.
- D. They are stateless and deny all inbound traffic by default.

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which statement describes security groups?

- A. They are stateful and allow all inbound traffic by default.
- B. They are stateful and deny all inbound traffic by default.
- C. They are stateless and allow all inbound traffic by default.
- D. They are stateless and deny all inbound traffic by default.

Knowledge check answer 2



154

Which statement describes security groups?

- A. They are stateful and allow all inbound traffic by default.
- B. **They are stateful and deny all inbound traffic by default. (correct)**
- C. They are stateless and allow all inbound traffic by default.
- D. They are stateless and deny all inbound traffic by default.

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **B. Security groups are stateful and deny all inbound traffic by default.**

Security groups are stateful. This means that they use previous traffic patterns and flows when evaluating new requests for an instance.

By default, security groups deny all inbound traffic, but you can add custom rules to fit your operational and security needs.

Knowledge check question 3



155

Which component is used to connect a VPC to the internet?

- A. Internet gateway
- B. Public subnet
- C. Edge location
- D. Security group

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which component is used to connect a VPC to the internet?

- A. Internet gateway
- B. Public subnet
- C. Edge location
- D. Security group

Knowledge check answer 3



156.

Which component is used to connect a VPC to the internet?

- A. **Internet gateway (correct)**
- B. Public subnet
- C. Edge location
- D. Security group

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is. **A. Internet gateway.**

The other response options are incorrect because:

- B. A public subnet is a section of a VPC that contains public-facing resources.
- C. An edge location is a site that Amazon CloudFront uses to store cached copies of your content for faster delivery to customers.
- D. A security group is a virtual firewall that controls inbound and outbound traffic for an Amazon EC2 instance.

Knowledge check question 4



157

Which service is used to manage the DNS records for domain names?

- A. Amazon Virtual Private Cloud
- B. AWS Direct Connect
- C. Amazon CloudFront
- D. Amazon Route 53

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which service is used to manage the DNS records for domain names?

- A. Amazon Virtual Private Cloud
- B. AWS Direct Connect
- C. Amazon CloudFront
- D. Amazon Route 53

Knowledge check answer 4



158.

Which service is used to manage the DNS records for domain names?

- A. Amazon Virtual Private Cloud
- B. AWS Direct Connect
- C. Amazon CloudFront
- D. **Amazon Route 53 (correct)**

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **D. Amazon Route 53**.

Amazon Route 53 is a DNS web service. It gives developers and businesses a reliable way to route end users to internet applications that host in AWS.

Another feature of Route 53 is the ability to manage the DNS records for domain names. You can transfer DNS records for existing domain names managed by other domain registrars. You can also register new domain names directly in Route 53.

The other response options are incorrect because:

- A. Amazon Virtual Private Cloud (Amazon VPC) is a service that enables you to provision an isolated section of the AWS Cloud. In this isolated section, you can launch resources in a virtual network that you define.
- B. AWS Direct Connect is a service that enables you to establish a dedicated private connection between your data center and VPC.
- C. Amazon CloudFront is a content delivery service. It uses a network of edge

locations to cache content and deliver content to customers all over the world.

Knowledge check question 5



159

Which statement describes DNS resolution?

- A. Launching resources in a customer-defined virtual network
- B. Storing local copies of content at edge locations around the world
- C. Connecting a VPC to the internet
- D. Translating a domain name to an IP address

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which statement describes DNS resolution?

- A. Launching resources in a customer-defined virtual network
- B. Storing local copies of content at edge locations around the world
- C. Connecting a VPC to the internet
- D. Translating a domain name to an IP address

Knowledge check answer 5



160

Which statement describes DNS resolution?

- A. Launching resources in a customer-defined virtual network
- B. Storing local copies of content at edge locations around the world
- C. Connecting a VPC to the internet
- D. **Translating a domain name to an IP address (correct)**

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **D. Translating a domain name to an IP address.**

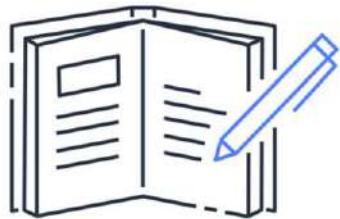
For example, if you want to visit AnyCompany's website, you enter the domain name into your PC and this request is sent to a DNS server. Next, the DNS server asks the web server for the IP address that corresponds to AnyCompany's website. The web server responds by providing the IP address for AnyCompany's website, 192.0.2.0.

Module 4 summary



In this module, you learned about:

- Structuring and connecting to a VPC
- Securing VPC resources with network access control lists and security groups
- Using Amazon Route 53 and Amazon CloudFront to deliver content



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

161

In this module, you learned about several tools for structuring and connecting to a VPC, including:

- Public and private subnets
- Internet gateways
- Virtual private gateways
- AWS Direct Connect

You also explored methods for securing VPC resources with network access control lists and security groups.

Finally, you examined how to use Amazon Route 53 with Amazon CloudFront to deliver content to your customers.

In the next module, you will explore AWS storage and database services.

Module 5

Storage and Databases



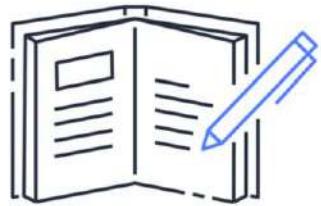
In this module, you will learn about storage and database types, their specific use cases, and their benefits.

Module 5 objectives



In this module, you will learn how to:

- Summarize the basic concept of storage and databases
- Describe Amazon Elastic Block Store (Amazon EBS) benefits
- Describe Amazon Simple Storage Service (Amazon S3) benefits
- Describe Amazon Elastic File System (Amazon EFS) benefits
- Summarize various storage solutions
- Describe Amazon Relational Database Service (Amazon RDS) benefits
- Describe Amazon DynamoDB benefits
- Summarize various database services



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

163

In this module, you will learn how to:

- Summarize the basic concept of storage and databases
- Describe Amazon Elastic Block Store (Amazon EBS) benefits
- Describe Amazon Simple Storage Service (Amazon S3) benefits
- Describe Amazon Elastic File System (Amazon EFS) benefits
- Summarize various storage solutions
- Describe Amazon Relational Database Service (Amazon RDS) benefits
- Describe Amazon DynamoDB benefits
- Summarize various database services

AWS storage

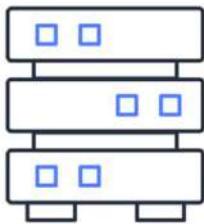
© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



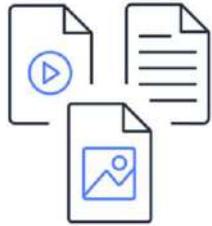
In previous modules, we've explored several areas of computing that are involved with running applications, such as CPU, memory, and networking. This module begins by focusing on another aspect of computing: storage.

The type of storage that you select for your applications can vary, based on your business and operational needs. For example, the coffee shop owners might need to store different types of data to support their applications. Examples include temporary test files, photos displayed on the coffee shop's website, and financial transaction records.

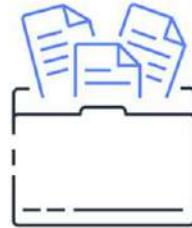
AWS storage types



Block storage



Object storage



File storage

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

105

This module explores three types of storage: block storage, object storage, and file storage.

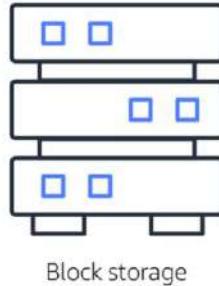
You will learn about AWS services that offer each type of storage and discuss how these services are used.

To begin, you will learn about block storage.

Block storage



- In **block storage**, files are separated into equal-sized pieces (blocks) of data.
- Block storage is used for applications that run on Amazon EC2 instances.

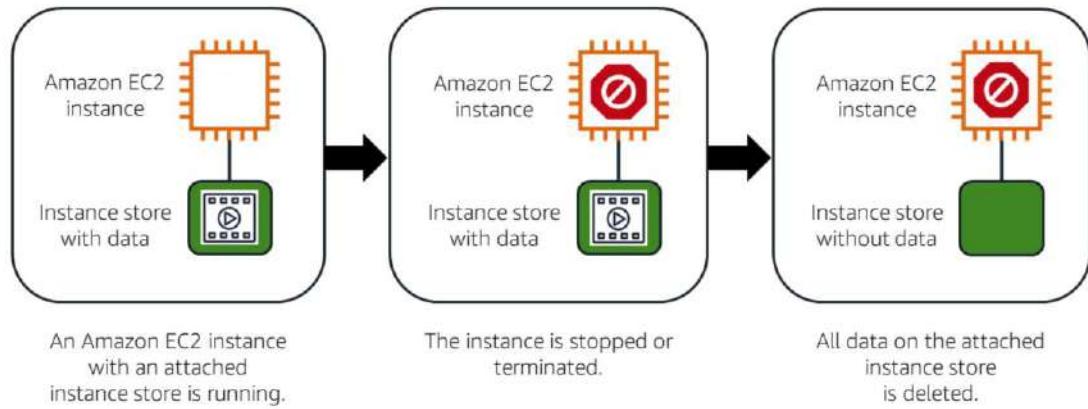


Block-level storage volumes behave like physical hard drives. In block storage, files are separated into equal-sized pieces (or blocks) of data. When a file in block storage is modified, only the pieces that are changed are updated.

Use block storage in a number of places such as databases, enterprise software applications, and computer hard drives. For example, suppose that you make a change to a single file on your computer's hard drive. Only the blocks for that file are updated. All of the blocks across the hard drive remain unchanged.

You can also use block storage for applications that run on Amazon EC2 instances. One type of block storage that you can use with Amazon EC2 instances is an **instance store**.

Instance store



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

107

An **instance store** provides temporary block-level storage for an Amazon EC2 instance. If you stop or terminate an Amazon EC2 instance, all the data written to the attached instance store is deleted.

Suppose that you are working on a document on your computer. You can think of an instance store as a working copy of the document. While you are working on the document, all the information is there. You can review the document, copy and paste information from the document, and so on. However, if you turn off your computer without saving the document, the document will no longer be there when you turn on the computer again.

Recall that Amazon EC2 instances are virtual servers. If you start an instance from a stopped state, the instance may start on another host, where the previously used instance store volume does not exist. Therefore, AWS recommends instance stores for use cases that involve temporary data that you do not need in the long term.

If you are working with data that needs retention, you can store it in **Amazon Elastic Block Store (Amazon EBS)** volumes.

Amazon EBS volumes



An Amazon EC2 instance with an attached EBS volume is running.

The instance is stopped or terminated. (If terminated, the EBS volume is removed by default.)

All data on the attached EBS volume remains available.

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

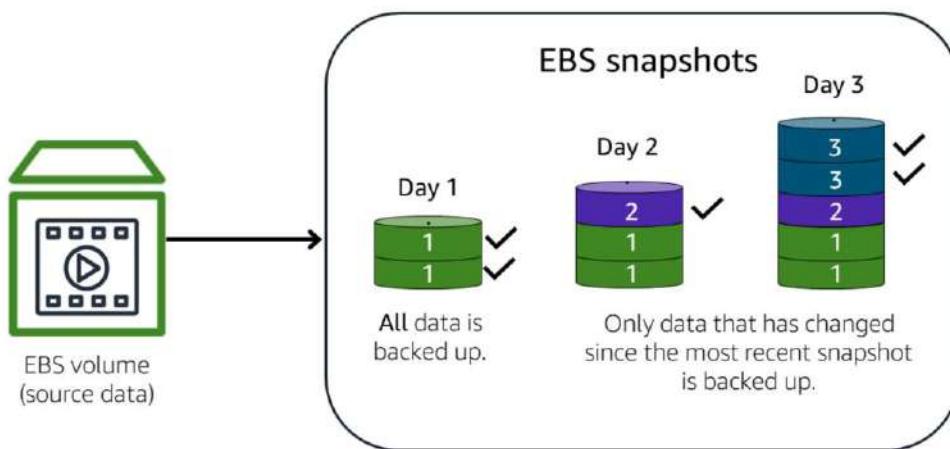
108

Amazon Elastic Block Store (Amazon EBS) is a service that provides block-level storage volumes that you can use with Amazon EC2 instances. If you stop or terminate an Amazon EC2 instance, all the data on the attached EBS volume remains available.

To create an EBS volume, you define the configuration (such as volume size and type) and provision it. After you create an EBS volume, it can attach to an Amazon EC2 instance.

Because EBS volumes are intended for data that needs to persist, it's important to back up the data. You can take incremental backups of EBS volumes by creating Amazon EBS snapshots.

Amazon EBS snapshots



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

108

An **Amazon EBS snapshot** is an incremental backup. This means that the first backup taken of a volume copies all the data. For subsequent backups, only the blocks of data that have changed since the most recent snapshot are saved.

Incremental backups are different from full backups, in which *all* the data in a storage volume copies each time a backup occurs. The backup includes data that has not changed since the most recent backup.

Later in this course, you will learn about Amazon CloudWatch. It is a service that you can use with Amazon EBS to automatically create Amazon EBS snapshots on a regular schedule.

Knowledge check



170

What are the differences between instance stores and Amazon EBS volumes?

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

What are the differences between instance stores and Amazon EBS volumes?

Knowledge check



- Instance stores are ideal for temporary data not kept long term.
- Amazon EBS volumes are ideal for data that requires retention.

Instance stores are ideal for temporary data that is not kept long term. When stopping or terminating an Amazon EC2 instance, all the data written to the attached instance store is deleted.

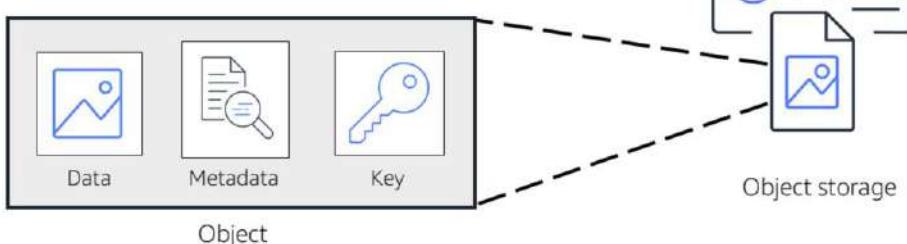
Amazon EBS volumes are ideal for data that requires retention. When stopping or terminating an Amazon EC2 instance, all the data on the attached EBS volume remains available.

The next type of storage that you will explore is object storage.

Object storage



In **object storage**, each object consists of data, metadata, and a key.



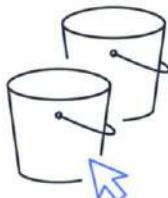
In **object storage**, each object consists of data, metadata, and a key.

The data might be an image, video, text document, or any other type of file. Metadata contains contextual information about what the data is, what it should be used for, the object size, and so on. An object's key is its unique identifier. For example, an object key name might be “4my-organization” or “my.great_photos-2014/jan/myvacation.jpg.”

Recall that when you modify a file in block storage, only the pieces that are changed are updated. When a file in object storage is modified, the entire object is updated.

To learn more about object storage, you need to examine **Amazon Simple Storage Service (Amazon S3)**.

Amazon Simple Storage Service



Store objects in buckets



Set permissions to control access to objects



Choose from a range of storage classes for different use cases

Amazon Simple Storage Service (Amazon S3) is a service that provides object-level storage. Amazon S3 stores data as objects within buckets.

You can upload any type of file to Amazon S3, such as images, videos, text files, and so on. For example, you might use Amazon S3 to store backup files, media files for a website, or archived documents. Amazon S3 offers unlimited storage space. The maximum file size for an object in Amazon S3 is 5 TB.

When you upload a file to Amazon S3, you can set permissions to control visibility and access to it. You can also use Amazon S3 versioning feature to track changes to your objects over time.

With Amazon S3, you pay only for what you use. You can choose from a range of storage classes to select a fit for your business and cost needs. When selecting an Amazon S3 storage class, consider these two factors:

- How often you plan to retrieve your data
- How available you need your data to be

Amazon S3 storage classes



S3 Standard

- Designed for frequently accessed data
- Stores data in a minimum of three Availability Zones

S3 Standard-IA

- Ideal for infrequently accessed data
- Similar to S3 Standard but has a lower storage price and higher retrieval price

S3 One Zone-IA

- Stores data in a single Availability Zone
- Has a lower storage price than S3 Standard-IA

The **S3 Standard** storage class provides high availability for objects. This makes it a good choice for a wide range of use cases, such as websites, content distribution, and data analytics. S3 Standard has a higher cost than other storage classes intended for infrequently accessed data and archival storage.

Suppose that some of the objects you are storing in Amazon S3 are backup files and accessed rarely. However, you still want to ensure that when you need the backup files, you can access them quickly.

<click> For this type of scenario, **S3 Standard-Infrequent Access (S3 Standard-IA)** might be a good fit. S3 Standard-IA is ideal for data infrequently accessed but requires high availability when needed. Both S3 Standard and S3 Standard-IA store data in a minimum of three Availability Zones. S3 Standard-IA provides the same level of availability as S3 Standard but with a lower storage price and a higher retrieval price.

Compared to S3 Standard, S3 Standard-IA has a lower per-TB storage price. Here's an example of what this means: Suppose that you have a few objects that you access only once a month. If you stored these objects in the S3 Standard storage class, you would pay a higher storage price for objects that are suited for S3 Standard-IA.

Compared to S3 Standard, S3 Standard-IA has a higher per-GB retrieval price. Suppose that you have a few objects that you need to frequently access throughout the day. S3 Standard-IA would most likely not be the optimal choice for these objects. You would pay a higher per-GB retrieval price as data is frequently accessed throughout the day. In this example, S3 Standard would be more cost-efficient.

<click> Another storage class to consider for infrequently accessed data is **S3 One Zone-Infrequent Access (S3 One Zone-IA)**. S3 One Zone-IA is ideal for infrequently accessed data that does not require high availability.

Compared to S3 Standard and S3 Standard-IA, which store data in a minimum of three Availability Zones, S3 One Zone-IA stores data in a single Availability Zone. This makes it a good storage class to consider if the following conditions apply:

- You want to save costs on storage
- You do not require the higher availability that S3 Standard and S3 Standard-IA offer

Amazon S3 storage classes



S3 Intelligent-Tiering

- Ideal for data with unknown or changing access patterns
- Requires a small monthly monitoring and automation fee per object

S3 Glacier

- Low-cost storage designed for data archiving
- Able to retrieve objects within a few minutes to hours

S3 Glacier Deep Archive

- Lowest-cost object storage class
- Able to retrieve objects within 12 hours

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

125

The scenarios discussed involved objects with access patterns that are known and consistent. If you have data with access patterns that are unknown or changing, you might consider storing this data in the **S3 Intelligent-Tiering** storage class.

In the S3 Intelligent-Tiering storage class, Amazon S3 monitors objects' access patterns. If you haven't accessed an object for 30 consecutive days, Amazon S3 automatically moves it to the infrequent access tier, S3 Standard-IA. If you access an object in the infrequent access tier, Amazon S3 automatically moves it to the frequent access tier, S3 Standard.

With S3 Intelligent-Tiering, there is a small monthly monitoring and automation fee per object. However, a key benefit of the S3 Intelligent-Tiering storage class is the ability to save time by not having to manually monitor your objects' access patterns. You also do not have to manually move them to different storage classes.

<click> The final Amazon S3 storage classes are **Amazon S3 Glacier** and **S3 Glacier Deep Archive**. These are low-cost storage classes that are ideal for data archiving. For example, you might use these storage classes to store archived customer records or earlier photos and video files.

When deciding between Amazon S3 Glacier and Amazon S3 Glacier Deep Archive, consider how quickly you must retrieve archived objects. You can retrieve objects stored in the Amazon S3 Glacier storage class within a few minutes to a few hours. By comparison, you can retrieve objects stored in the S3 Glacier Deep Archive storage class within 12 hours.

Next, you will review the Amazon S3 storage classes.

Knowledge check



175

You want to store data that is infrequently accessed but must be immediately available when needed. Which Amazon S3 storage class should you use?

- A. S3 Intelligent-Tiering
- B. S3 Glacier Deep Archive
- C. S3 Standard-IA
- D. S3 Glacier

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

You want to store data that is infrequently accessed but must be immediately available when needed. Which Amazon S3 storage class should you use?

- A. S3 Intelligent-Tiering
- B. S3 Glacier Deep Archive
- C. S3 Standard-IA
- D. S3 Glacier

Knowledge check



177

You want to store data that is infrequently accessed but must be immediately available when needed. Which Amazon S3 storage class should you use?

- A. S3 Intelligent-Tiering
- B. S3 Glacier Deep Archive
- C. **S3 Standard-IA (correct)**
- D. S3 Glacier

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **C. S3 Standard-IA**.

The S3 Standard-IA storage class is ideal for data that is infrequently accessed but requires high availability when needed. Both S3 Standard and S3 Standard-IA store data in a minimum of three Availability Zones. S3 Standard-IA provides the same level of availability as S3 Standard but at a lower storage price.

The other response options are incorrect because:

- In the S3 Intelligent-Tiering storage class, Amazon S3 monitors objects' access patterns. If you haven't accessed an object for 30 consecutive days, Amazon S3 automatically moves it to the infrequent access tier, S3 Standard-IA. If you access an object in the infrequent access tier, Amazon S3 automatically moves it to the frequent access tier, S3 Standard.
- S3 Glacier and S3 Glacier Deep Archive are low-cost storage classes that are ideal for data archiving. They would not be the best choice for this scenario, which requires high availability. You can retrieve objects stored in the S3 Glacier storage class within a few minutes to a few hours. By comparison, you can retrieve objects

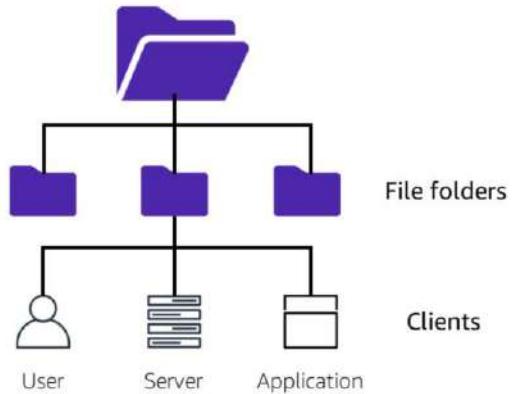
stored in the S3 Glacier Deep Archive storage class within 12 hours.

Next, you will examine the third type of storage: file storage.

File storage



In **file storage**, multiple clients can access data that is stored in shared file folders.



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

178

Suppose that your company has a large amount of data needing access by many users or applications simultaneously. For example, this data might connect to multiple servers that are constantly performing analytics on it.

In **file storage**, multiple clients (such as users, applications, servers, and so on) can access data that is stored in shared file folders. In this approach, a storage server uses block storage with a local file system to organize files. Clients access data through file paths.

Compared to block storage and object storage, file storage is ideal for use cases in which a large number of services and resources need to access the same data at the same time.

Next you will examine **Amazon Elastic File System (Amazon EFS)**, a service that provides file storage.

Amazon Elastic File System



Store data in a scalable file system



Provide data to thousands of Amazon EC2 instances concurrently



Store data in and across multiple Availability Zones

Amazon Elastic File System (Amazon EFS) is a scalable file system used with AWS Cloud services and on-premises resources. As you add and remove files, Amazon EFS grows and shrinks automatically. It can scale on demand to petabytes without disrupting applications.

Suppose that multiple applications need access to your data in Amazon EFS at the same time, but without affecting the applications' performance. Thousands of Amazon EC2 instances can access Amazon EFS concurrently.

One of the differences between Amazon EBS and Amazon EFS is how the two services work within and across Availability Zones. Amazon EBS volumes are an *Availability Zone-level* resource. An EBS volume stores data within a single Availability Zone. To attach an Amazon EC2 instance to an EBS volume, both the Amazon EC2 instance and the EBS volume must reside within the same Availability Zone.

By contrast, Amazon EFS is a *Regional* service. It stores data within and across multiple Availability Zones. This allows data to be accessed concurrently from all the Availability Zones in the Region where a file system is located. Additionally, on-premises servers are able to access Amazon EFS by using AWS Direct Connect.

AWS databases

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



This section explores AWS database services. To learn about the types of databases, you will look at two examples from the coffee shop.

Database types



Relational database

ID	Product name	Size	Price
1	Medium roast ground coffee	12 oz.	\$5.30
2	Dark roast ground coffee	20 oz.	\$9.27

Nonrelational database

Key	Value
1	Name: John Doe Address: 123 Any Street Favorite drink: Medium latte
2	Name: Mary Major Address: 100 Main Street Birthday: July 5, 1994

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

101

The coffee shop has been ordering several new products from its distributors, but employees are finding it difficult to keep up with the entire new inventory. To fix this issue, the coffee shop owners plan to create an inventory management system.

Additionally, the coffee shop has been getting many frequent customers, so the owners decide to create a digital rewards application. The owners must track information such as the drinks that customers order and the amounts that customers spend.

In the process of designing the new inventory management system and rewards application, the coffee shop owners decide to use **databases**. A database is an organized collection of structured information.

The coffee shop owners need to ensure that they are choosing the right type of databases for their two different use cases. As with the storage services you learned about, AWS offers a variety of database services to support different business needs.

The database types are relational databases and nonrelational databases.

Relational databases



- In a **relational database**, data is stored in a way that relates it to other pieces of data.
- Relational databases use **structured query language (SQL)** to store and query data.

ID	Product name	Size	Price
1	Medium roast ground coffee	12 oz.	\$5.30
2	Dark roast ground coffee	20 oz.	\$9.27

Example of data in a relational database

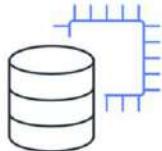
In a **relational database**, data is stored in a way that relates it to other pieces of data.

An example of a relational database might be the coffee shop's inventory management system. Each record in the database would include data for a single item, such as product name, size, price, and so on.

Relational databases use **structured query language (SQL)** to store and query data. This approach allows data to be stored in an easily understandable, consistent, and scalable way. For example, the coffee shop owners can write a SQL query to identify all the customers whose most frequently purchased drink is a medium latte.

You can learn more about relational databases by examining **Amazon Relational Database Service (Amazon RDS)**.

Amazon Relational Database Service



Operate and scale a relational database in the AWS Cloud



Automate time-consuming administrative tasks



Store and transmit data securely

Amazon Relational Database Service (Amazon RDS) is a service that allows you to run relational databases in the AWS Cloud.

Amazon RDS is a managed service that automates tasks such as hardware provisioning, database setup, patching, and backups. With these capabilities, you can spend less time completing administrative tasks and more time using data to innovate your applications. You can integrate Amazon RDS with other services to fulfill your business and operational needs, such as using AWS Lambda to query your database from a serverless application.

Amazon RDS provides a number of different security options. Many Amazon RDS database engines offer encryption at rest (protecting data while it is stored) and encryption in transit (protecting data while it is being sent and received).

Amazon RDS database engines



- Amazon Aurora
- PostgreSQL
- MySQL
- MariaDB
- Oracle Database
- Microsoft SQL Server



Amazon RDS

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

104

Amazon RDS is available on six database engines, which optimize for memory, performance, or input/output (I/O). The database engines include:

- Amazon Aurora
- PostgreSQL
- MySQL
- MariaDB
- Oracle Database
- Microsoft SQL Server

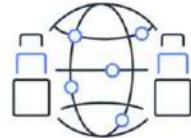
Amazon Aurora



Store data in an enterprise-class relational database



Reduce database costs by eliminating unnecessary input/output (I/O) operations



Replicate six copies of data across three Availability Zones

Amazon Aurora is an enterprise-class relational database. It is compatible with MySQL and PostgreSQL relational databases. It is up to five times faster than standard MySQL databases and up to three times faster than standard PostgreSQL databases.

Amazon Aurora helps to reduce your database costs by reducing unnecessary input/output (I/O) operations, while ensuring that your database resources remain reliable and available.

Consider Amazon Aurora if your workloads require high availability. It replicates six copies of your data across three Availability Zones, and continuously backs up your data to Amazon S3.



Discussion

One of the employees at the coffee shop has an idea for the new inventory management system. They believe they should maintain data in a text file in Amazon S3.

Do you agree with their suggestion?

Why or why not?

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



Instructor note

This discussion provides learners with an opportunity to consider the differences between when to store data in object storage or in a database. Some benefits to mention about relational databases include the ability to store and query data in a structured and consistent format, and the ability to integrate databases with other AWS services.

One of the employees at the coffee shop has an idea for the new inventory management system.

They believe you should maintain data in a text file in Amazon S3.

Do you agree with their suggestion? Why or why not?

Nonrelational databases



- A **nonrelational database** uses structures other than rows and columns to organize data.
- For example, with **key-value pairs**, data is organized into items (keys), and items have attributes (values).

Key	Value
1	Name: John Doe Address: 123 Any Street Favorite drink: Medium latte
2	Name: Mary Major Address: 100 Main Street Birthday: July 5, 1994

Example of data in a nonrelational database

Depending on your business needs, you might also consider storing data in a **nonrelational database**.

In a nonrelational database, you create tables. A table is a place where you can store and query data.

Some refer to nonrelational databases as “NoSQL databases” because they use structures other than rows and columns to organize data. One type of structural approach for nonrelational databases is **key-value pairs**. With key-value pairs, data is organized into items (keys), and items have attributes (values). You can think of attributes as being different features of your data.

For example, the coffee shop might use a key-value database to organize all of its customer information for the rewards application. This database could include data pairs such as “Name: John Doe,” “Address: 123 Any Street,” “City: Anytown,” and so on.

In a key-value database, you can add or remove attributes from items in the table at any time. Additionally, not every item in the table has to have the same attributes.

To learn more about nonrelational databases, explore Amazon DynamoDB.

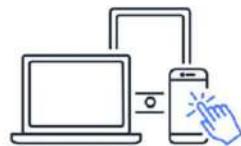
Amazon DynamoDB



Amazon DynamoDB is a serverless key-value database.



It automatically scales to adjust for capacity changes and maintain consistent performance.



It is designed to handle over 10 trillion requests per day.

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

100

Amazon DynamoDB is a key-value database service. It delivers single-digit millisecond performance at any scale.

DynamoDB is serverless, which means that you do not have to provision, patch, or manage servers. You also do not have to install, maintain, or operate software.

As the size of your database shrinks or grows, DynamoDB automatically scales to adjust for changes in capacity while maintaining consistent performance. This makes it a suitable choice for use cases that require high performance while scaling. For example, the coffee shop is adding many new customers into its database every day. It needs a database solution that can continue to provide high performance while automatically scaling. For this reason, the coffee shop owners decide to run their customer database in DynamoDB.

The coffee shop owners also must ensure that the database can handle an increase in requests during their popular promotional events. DynamoDB would be a good choice for this use case because it can handle more than 10 trillion requests per day and support peaks of more than 20 million requests per second.

Here's an example of DynamoDB's scaling capabilities: During the Amazon Prime Day event in 2019, which lasted 48 hours, there were 7.11 trillion requests made to the DynamoDB API. This peaked at 45.4 million requests per second.

What if you already have an existing database that you want to move into the AWS Cloud? For both relational and nonrelational databases, you can use **AWS Database Migration Service (AWS DMS)**.

AWS Database Migration Service



Migrate relational databases, nonrelational databases, and other types of data stores

Example



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

109

AWS Database Migration Service (AWS DMS) allows you to migrate relational databases, nonrelational databases, and other types of data stores.

With AWS DMS, you move data between a source database and a target database. The source and target databases can be of the same type or different types. During the migration, your source database remains operational, reducing downtime for any applications that rely on the database.

For example, you have a MySQL database that is stored on premises in an Amazon EC2 instance or in Amazon RDS. The MySQL database would be considered your source database. Using AWS DMS, you could migrate your data to a target database, such as an Amazon Aurora database.

Other use cases for AWS DMS include:

- **Development and test database migrations** – Enabling developers to test applications against production data but without affecting production users.
- **Database consolidation** – Combining several databases into a single database.

- **Continuous replication** – Sending ongoing copies of your data to other target sources instead of doing a one-time migration.

Amazon RDS and Amazon DynamoDB



For each scenario, should you use **Amazon RDS** or **Amazon DynamoDB**?

Amazon RDS

1. Storing data in a relational database

DynamoDB

3. Storing data in a key-value database

DynamoDB

5. Scaling up to 10 trillion requests per day

2. Running a serverless database

DynamoDB

4. Using SQL to organize data

Amazon RDS

6. Storing data in an Amazon Aurora database

Amazon RDS

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

190

Animation note: Click once for each question and answer.

Instructor Note:

This is a quick quiz to keep the audience engaged and test their understanding of the differences between when to use Amazon RDS and Amazon DynamoDB. If they get any answer wrong, use that opportunity to clarify why the answer is a wrong one.

For each situation, determine whether Amazon RDS or Amazon DynamoDB would be the better database service to use. Items filled in with purple are sample use cases for Amazon RDS; those that are filled in with pink are sample use cases for Amazon DynamoDB.

Additional database services

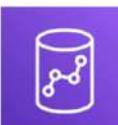
© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



Throughout this module, you have learned how to select storage and database services for various use cases.

Next, you will briefly examine some additional database services used to fulfill your company's business and operational needs. These additional services are described at a high level.

Additional database services



Amazon Redshift

Query and analyze data across a data warehouse



Amazon DocumentDB

Run MongoDB workloads in a document database service



Amazon Neptune

Run applications that use highly connected datasets



Amazon QLDB

Review a complete history of changes to your application data

Amazon Redshift is a data warehousing service that you can use for big data analytics. It offers the ability to collect data from many sources and help you to understand relationships and trends across your data.

Amazon DocumentDB is a document database service that supports MongoDB workloads. (MongoDB is a document database program.)

Amazon Neptune is a graph database service. You can use Amazon Neptune to build and run applications that work with highly connected datasets, such as recommendation engines, fraud detection, and knowledge graphs.

Amazon Quantum Ledger Database (Amazon QLDB) is a ledger database service. You can use Amazon QLDB to review a complete history of all the changes that have been made to your application data.

Additional database services



Amazon Managed Blockchain

Run a decentralized ledger database



Amazon ElastiCache

Add caching layers to improve database read times



Amazon DynamoDB Accelerator

Improve DynamoDB response times from single-digit milliseconds to microseconds

Amazon Managed Blockchain is a service that you can use to create and manage blockchain networks with open-source frameworks. Blockchain is a distributed ledger system that lets multiple parties run transactions and share data without a central authority.

If you must make your databases run faster, consider using **Amazon ElastiCache**. Amazon ElastiCache is a service that adds caching layers on top of your databases to help improve the read times of common requests. It supports two types of data stores: Redis and Memcached.

Finally, **Amazon DynamoDB Accelerator (DAX)** is an in-memory cache for DynamoDB. It helps improve response times from single-digit milliseconds to microseconds.

Module 5

Knowledge check

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



Knowledge check question 1



195

Which Amazon S3 storage classes are optimized for archival data? (Select TWO.)

- A. S3 Standard
- B. S3 Glacier
- C. S3 Intelligent-Tiering
- D. S3 Glacier Deep Archive
- E. S3 Standard-IA

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which Amazon S3 storage classes are optimized for archival data? (Select TWO.)

- A. S3 Standard
- B. S3 Glacier
- C. S3 Intelligent-Tiering
- D. S3 Glacier Deep Archive
- E. S3 Standard-IA

Knowledge check answer 1



195.

Which Amazon S3 storage classes are optimized for archival data? (Select TWO.)

- A. S3 Standard
- B. **S3 Glacier (correct)**
- C. S3 Intelligent-Tiering
- D. **S3 Glacier Deep Archive (correct)**
- E. S3 Standard-IA

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct two response options are:

- B. S3 Glacier**
- D. S3 Glacier Deep Archive**

Objects stored in the S3 Glacier storage class can be retrieved within a few minutes to a few hours. By comparison, objects that are stored in the S3 Glacier Deep Archive storage class can be retrieved within 12 hours.

The other response options are incorrect because:

A – S3 Standard is a storage class that is ideal for frequently accessed data, not archival data.

C – S3 Intelligent-Tiering monitors access patterns of objects and automatically moves them between the S3 Standard and S3 Standard-IA storage classes. It is not designed for archival data.

E – S3 Standard-IA is ideal for data that is infrequently accessed but requires high

availability when needed.

Knowledge check question 2



197

Which option is TRUE about Amazon EBS volumes and Amazon EFS file systems?

- A. EBS volumes store data in a single Availability Zone. Amazon EFS file systems store data across multiple Availability Zones.
- B. EBS volumes store data across multiple Availability Zones. Amazon EFS file systems store data in a single Availability Zone.
- C. EBS volumes and Amazon EFS file systems both store data in a single Availability Zone.
- D. EBS volumes and Amazon EFS file systems both store data across multiple Availability Zones.

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which statement or statements are TRUE about Amazon EBS volumes and Amazon EFS file systems?

- A. EBS volumes store data within a single Availability Zone. Amazon EFS file systems store data across multiple Availability Zones.
- B. EBS volumes store data across multiple Availability Zones. Amazon EFS file systems store data within a single Availability Zone.
- C. EBS volumes and Amazon EFS file systems both store data within a single Availability Zone.
- D. EBS volumes and Amazon EFS file systems both store data across multiple Availability Zones.

Knowledge check answer 2



198

Which option is TRUE about Amazon EBS volumes and Amazon EFS file systems?

- A. EBS volumes store data in a single Availability Zone. Amazon EFS file systems store data across multiple Availability Zones. (correct)
- B. EBS volumes store data across multiple Availability Zones. Amazon EFS file systems store data in a single Availability Zone.
- C. EBS volumes and Amazon EFS file systems both store data in a single Availability Zone.
- D. EBS volumes and Amazon EFS file systems both store data across multiple Availability Zones.

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **A. EBS volumes store data within a single Availability Zone. Amazon EFS file systems store data across multiple Availability Zones.**

An EBS volume must be located in the same Availability Zone as the Amazon EC2 instance to which it is attached.

Data in an Amazon EFS file system can be accessed concurrently from all the Availability Zones in the Region where the file system is located.

Knowledge check question 3



199

A customer wants to store data in an object storage service. Which AWS service should the customer use for this type of storage?

- A. Amazon Managed Blockchain
- B. Amazon Elastic File System (Amazon EFS)
- C. Amazon Elastic Block Store (Amazon EBS)
- D. Amazon Simple Storage Service (Amazon S3)

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

A customer wants to store data in an object storage service. Which AWS service should the customer use for this type of storage?

- A. Amazon Managed Blockchain
- B. Amazon Elastic File System (Amazon EFS)
- C. Amazon Elastic Block Store (Amazon EBS)
- D. Amazon Simple Storage Service (Amazon S3)

Knowledge check answer 3



200

A customer wants to store data in an object storage service. Which AWS service should the customer use for this type of storage?

- A. Amazon Managed Blockchain
- B. Amazon Elastic File System (Amazon EFS)
- C. Amazon Elastic Block Store (Amazon EBS)
- D. **Amazon Simple Storage Service (Amazon S3) (correct)**

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **D. Amazon Simple Storage Service (Amazon S3)**.

The other response options are incorrect because:

- A. Amazon Managed Blockchain is a service that you can use to create and manage blockchain networks with open-source frameworks. Blockchain is a distributed ledger system that lets multiple parties run transactions and share data without a central authority.
- B. Amazon Elastic File System (Amazon EFS) is a scalable file system used with AWS Cloud services and on-premises resources. It does not store data as object storage.
- C. Amazon Elastic Block Store (Amazon EBS) is a service that provides block-level storage volumes that you can use with Amazon EC2 instances.

Knowledge check question 4



201

Which statement describes Amazon DynamoDB?

- A. A service that allows customers to run relational databases in the AWS Cloud
- B. A serverless key-value database service
- C. A service that customers can use to migrate relational databases, nonrelational databases, and other types of data stores
- D. An enterprise-class relational database

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which statement best describes Amazon DynamoDB?

- A. A service that allows customers to run relational databases in the AWS Cloud
- B. A serverless key-value database service
- C. A service that customers can use to migrate relational databases, nonrelational databases, and other types of data stores
- D. An enterprise-class relational database

Knowledge check answer 4



202

Which statement describes Amazon DynamoDB?

- A. A service that allows customers to run relational databases in the AWS Cloud
- B. **A serverless key-value database service (correct)**
- C. A service that customers can use to migrate relational databases, nonrelational databases, and other types of data stores
- D. An enterprise-class relational database

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **B. A serverless key-value database service.**

Amazon DynamoDB is a key-value database service. It is serverless, which means that you do not have to provision, patch, or manage servers.

The other response options are incorrect because:

- A. A service that allows you to run relational databases in the AWS Cloud describes Amazon Relational Database Service (Amazon RDS).
- C. A service that you can use to migrate relational databases, nonrelational databases, and other types of data stores describes AWS Database Migration Service (AWS DMS).
- D. An enterprise-class relational database describes Amazon Aurora.

Knowledge check question 5



205.

Which service is used to query and analyze data across a data warehouse?

- A. Amazon Neptune
- B. Amazon DocumentDB
- C. Amazon ElastiCache
- D. Amazon Redshift

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which service is used to query and analyze data across a data warehouse?

- A. Amazon Neptune
- B. Amazon DocumentDB
- C. Amazon ElastiCache
- D. Amazon Redshift

Knowledge check answer 5



204

Which service is used to query and analyze data across a data warehouse?

- A. Amazon Neptune
- B. Amazon DocumentDB
- C. Amazon ElastiCache
- D. **Amazon Redshift (correct)**

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **D. Amazon Redshift**.

Amazon Redshift is a data warehousing service that you can use for big data analytics. Use Amazon Redshift to collect data from many sources and help you understand relationships and trends across your data.

The other response options are incorrect because:

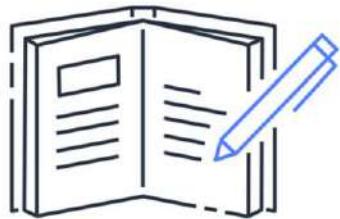
- A. Amazon Neptune is a graph database service. You can use Amazon Neptune to build and run applications that work with highly connected datasets, such as recommendation engines, fraud detection, and knowledge graphs.
- B. Amazon DocumentDB is a document database service that supports MongoDB workloads.
- C. Amazon ElastiCache is a service that adds caching layers on top of your databases to help improve the read times of common requests.

Module 5 summary



In this module, you learned about:

- AWS storage services and resources
- Amazon S3 storage classes
- AWS database services



In this module, you learned about AWS storage services and resources, including:

- Instance stores
- Amazon EBS
- Amazon S3
- Amazon EFS

You also learned about the six Amazon S3 storage classes:

- S3 Standard
- S3 Standard-Infrequent Access
- S3 One Zone-Infrequent Access
- S3 Intelligent-Tiering
- S3 Glacier
- S3 Glacier Deep Archive

Finally, you learned about AWS database services, including:

- Amazon RDS

- Amazon Aurora
- Amazon DynamoDB
- AWS DMS

In the next module, you will learn about AWS security services.

Module 6

Security



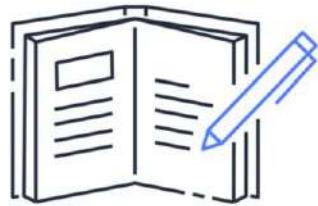
In this module, you will learn about security at AWS. This includes the shared responsibility model, AWS Identity and Access Management, AWS Organizations, and compliance.

Module 6 objectives



In this module, you will learn how to:

- Explain the benefits of the shared responsibility model
- Describe multi-factor authentication (MFA)
- Differentiate among the AWS Identity and Access Management (IAM) security levels
- Explain AWS Organizations benefits
- Describe security policies
- Summarize the benefits of compliance with AWS
- Explain additional AWS security services

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.207

In this module, you will learn how to:

- Explain the benefits of the shared responsibility model
- Describe multi-factor authentication (MFA)
- Differentiate between the AWS Identity and Access Management (IAM) security levels
- Explain the main benefits of AWS Organizations

Shared responsibility model

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



Throughout this course, you have learned about a variety of resources that you can create in the AWS Cloud. These resources include Amazon EC2 instances, Amazon S3 buckets, and Amazon RDS databases. Who is responsible for keeping these resources secure: you (the customer) or AWS?

The answer is **both**. The reason is that you do not treat your AWS environment as a single object. Rather, you treat the environment as a collection of parts that build upon each other. AWS is responsible for some parts of your environment and you (the customer) are responsible for other parts. This concept is known as the shared responsibility model.

Shared responsibility model



Customers	Customer Data		
	Platform, Applications, Identity and Access Management		
	Operating Systems, Network and Firewall Configuration		
	Client-side Data Encryption	Server-side Encryption	Networking Traffic Protection
AWS	Software		
	Compute	Storage	Database
	Hardware/AWS Global Infrastructure		
	Regions	Availability Zones	Edge Locations

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

209

The shared responsibility model divides into customer responsibilities (commonly referred to as “security *in* the cloud”) and AWS responsibilities (commonly referred to as “security *of* the cloud”).

You can think of this model as being similar to the division of responsibilities between a homeowner and a homebuilder. The builder (AWS) is responsible for constructing your house and ensuring that it is solidly built. As the homeowner (the customer), it is your responsibility to secure everything in the house by ensuring that the doors are closed and locked.

This section examines the shared responsibility model in greater detail, beginning with customers’ responsibilities.

Customers: Security IN the cloud



Customers	Customer Data		
	Platform, Applications, Identity and Access Management		
	Operating Systems, Network and Firewall Configuration		
	Client-side Data Encryption	Server-side Encryption	Networking Traffic Protection

Examples of customer responsibilities include:

- Instance operating system
- Applications
- Security groups
- Host-based firewalls
- Account management

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

310

Customers are responsible for the security of everything that they create and put *in* the AWS Cloud.

When using AWS services, you, the customer, maintain complete control over your content. You are responsible for managing security requirements for your content, including which content you choose to store on AWS, which AWS services you use, and who has access to that content. You also control how access rights are granted, managed, and revoked.

The security steps that you take will depend on factors such as the services that you use, the complexity of your systems, and your company's specific operational and security needs. Steps include selecting, configuring, and patching the operating systems that will run on Amazon EC2 instances, configuring security groups, and managing user accounts.

AWS: Security OF the cloud



AWS	Software			
	Compute	Storage	Database	Networking
	Hardware/AWS Global Infrastructure			
	Regions	Availability Zones		Edge Locations

Examples of AWS responsibilities include:

- Physical security of data centers
- Hardware and software infrastructure
- Network infrastructure
- Virtualization infrastructure

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

311

AWS is responsible for security *of* the cloud.

AWS operates, manages, and controls the components at all layers of infrastructure. This includes areas such as the host operating system, the virtualization layer, and even the physical security of the data centers from which services operate.

AWS is responsible for protecting the global infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure includes AWS Regions, Availability Zones, and edge locations.

AWS manages the security of the cloud, specifically the physical infrastructure that hosts your resources, which include:

- Physical security of data centers
- Hardware and software infrastructure
- Network infrastructure
- Virtualization infrastructure

Although you cannot visit AWS data centers to see this protection firsthand, AWS provides several reports from third-party auditors. These auditors have verified its compliance with a variety of computer security standards and regulations.

Review: Shared responsibility model



Are these tasks the responsibilities of **customers** or **AWS**?

Customers

1. Configuring security groups on Amazon EC2 instances

AWS

3. Implementing physical security controls at data centers

AWS

5. Maintaining servers that run Amazon EC2 instances

2. Maintaining network infrastructure

AWS

4. Patching software on Amazon EC2 instances

Customers

6. Setting permissions for Amazon S3 objects

Customers

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

312

Instructor notes

This is a quick quiz to keep the audience engaged and test their understanding of the AWS shared responsibility model. Click once for each question and answer.

If they get any answer wrong, use that opportunity to further clarify why the answer is a wrong one.

Suppose that you are the owner of the coffee shop. Each item on this slide represents an aspect of running the coffee shop's website. For each item, determine if it is your (the customer's) responsibility or an AWS responsibility.

Items that are filled in with orange are the responsibility of AWS; those that are filled in with blue are the responsibility of the customer.

AWS Identity and Access Management (IAM)

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



One area included in customers' responsibilities is identity and access management. You will explore this topic so you can understand the role that it plays in keeping your AWS resources secure.

Security in the coffee shop



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

214

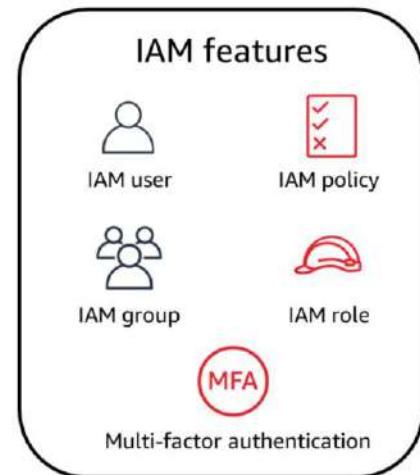
The coffee shop uses a computer system for its point of sale system, inventory system, and employee records. When a new employee begins working at the coffee shop, they are given their own account within the computer system.

Each employee's account has been assigned permissions that allow them to carry out only the tasks that relate to their specific job. For example, a cashier's account allows them to access the point of sale system, but not employee records or the inventory system.

This type of functionality also exists in AWS. To create user identities and assign permissions, you use **AWS Identity and Access Management (IAM)**.



AWS Identity and Access Management (IAM) allows you to manage access to AWS services and resources.



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

215

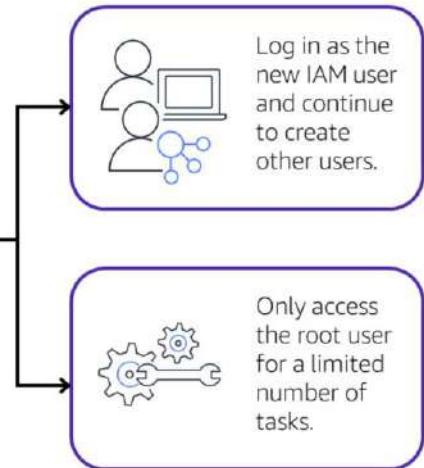
AWS Identity and Access Management (IAM) allows you to manage access to AWS services and resources securely.

IAM gives you the flexibility to configure access based on your company's specific operational and security needs. You do this by using a combination of IAM features, which are explored in detail in this lesson:

- IAM users, groups, and roles
- IAM policies
- Multi-factor authentication

You will also learn best practices for each of these features.

AWS account root user



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

216

When you first create an AWS account, you begin with an identity that is known as the **root user**.

The root user is accessed by signing in with the email address and password that you used to create your AWS account. You can think of the root user as being similar to the owner of the coffee shop. It has complete access to all of the AWS services and resources within the account.

<click> Do **not** use the root user for everyday tasks. Instead, use the root user to create your first IAM user and assign it permissions to create other users.

<click> Then, continue to create other IAM users, and access those identities for performing regular tasks throughout AWS. Only use the root user when you need to perform a limited number of tasks that are only available to the root user. Examples of these tasks include changing your root user email address and changing your AWS Support plan.

An **IAM user** is an identity that represents a person or application that interacts with AWS services and resources.

Best practice: Create individual IAM users for each person who needs to access AWS.



IAM user

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

217

An **IAM user** is an identity that you create in AWS. It represents the person or application that interacts with AWS services and resources. It consists of a name and credentials.

By default, when you create a new IAM user in AWS, it has no permissions associated with it. To allow the IAM user to perform specific actions in AWS, such as launching an Amazon EC2 instance or creating an Amazon S3 bucket, you must grant the IAM user the necessary permissions.

As a best practice, create individual IAM users for each person who must access AWS.

Even if you have multiple employees who require the same level of access, you should create individual IAM users for each of them. This provides additional security by allowing each IAM user to have a unique set of security credentials.

An **IAM policy** is a document that grants or denies permissions to AWS services and resources.

Best practice: Follow the security principle of least privilege.



IAM policy

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

218

An **IAM policy** is a document that allows or denies permissions to AWS services and resources.

IAM policies allow you to customize users' levels of access to resources. For example, you can allow users to access all of the Amazon S3 buckets within your AWS account, or only a specific bucket.

As a best practice, follow the security principle of **least privilege** when granting permissions.

By following this principle, you help to prevent users or roles from having more permissions than needed to perform their tasks.

For example, if an employee needs access to only a specific bucket, specify the bucket in the IAM policy. Do this instead of granting the employee access to all of the buckets in your AWS account.

Example: IAM policy



This sample IAM policy allows permission to access the objects in the Amazon S3 bucket with ID: *awsdoc-example-bucket*.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {"Effect": "Allow",  
         "Action": "s3>ListObject",  
         "Resource": "arn:aws:s3:::  
awsdoc-example-bucket"}  
    ]  
}
```

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

219

Here's an example of how IAM policies work. Suppose that the coffee shop owner has created an IAM user for a newly hired cashier. The cashier needs access to the receipts that are kept in an Amazon S3 bucket with the ID: *awsdoc-example-bucket*.

The coffee shop owner uses the following IAM policy to grant the cashier access to the *awsdoc-example-bucket* bucket in Amazon S3:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {"Effect": "Allow",  
         "Action": "s3>ListObject",  
         "Resource": "arn:aws:s3:::  
awsdoc-example-bucket"}  
    ]  
}
```

In this example, the IAM policy is allowing a specific action within Amazon S3: ListObject. The policy also mentions a specific bucket ID: *awsdoc-example-bucket*. When the owner attaches this policy to the cashier's IAM user, it will allow the

cashier to view all of the objects in the *awsdoc-example-bucket* bucket.

If the owner wants the cashier to be able to access other services and perform other actions in AWS, the owner must attach additional policies to specify these services and actions.

Now, suppose that the coffee shop has hired a few more cashiers. Instead of assigning permissions to each individual IAM user, the owner places the users into an **IAM group**.

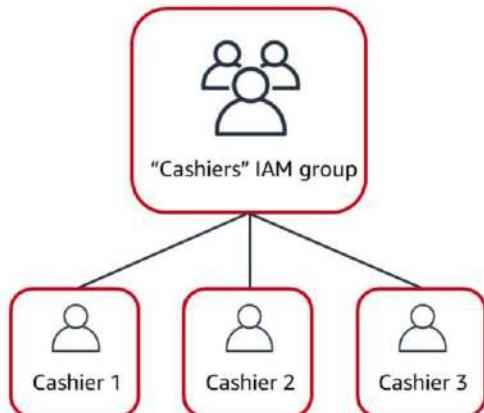
IAM groups



An **IAM group** is a collection of IAM users.

Best practice: Attach IAM policies to IAM groups, rather than to individual IAM users.

Members inherit the policies assigned to the group.



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

220

An **IAM group** is a collection of IAM users. When you assign an IAM policy to a group, all users in the group are granted permissions specified by the policy.

Here's an example of how this might work in the coffee shop. Instead of assigning permissions to cashiers one at a time, the owner can create a "Cashiers" IAM group. The owner can then add IAM users to the group and then attach permissions at the group level.

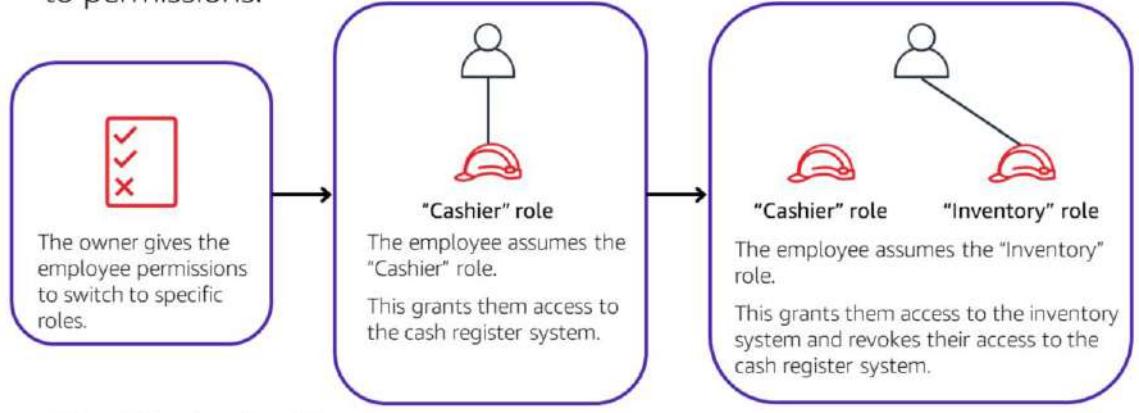
Assigning IAM policies at the group level also makes it easier to adjust permissions when an employee transfers to a different job. For example, if a cashier becomes an inventory specialist, the coffee shop owner removes them from the "Cashiers" IAM group and adds them into the "Inventory Specialists" IAM group. This ensures that employees have only the permissions that are required for their current role.

What if a coffee shop employee hasn't switched jobs permanently, but instead, rotates to different workstations throughout the day? This employee can get the access they need through **IAM roles**.

IAM roles



An **IAM role** is an identity that you can assume to gain temporary access to permissions.



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

221

In the coffee shop, an employee rotates to different workstations throughout the day. Depending on the staffing of the coffee shop, this employee might perform several duties: work at the cash register, update the inventory system, process online orders, and so on.

When the employee needs to switch to a different task, they give up their access to one workstation and gain access to the next workstation. The employee can easily switch between workstations, but at any given point in time, they can have access to only a single workstation. This same concept exists in AWS with **IAM roles**.

An IAM role is an identity that you can assume to gain temporary access to permissions.

Before an IAM user, application, or service can assume an IAM role, they must be granted permissions to switch to the role. When someone assumes an IAM role, they abandon all previous permissions that they had under a previous role and assume the permissions of the new role. (**Note:** When an IAM user is assuming a role, they remain logged into the AWS Management Console through their IAM user account and can switch back to their IAM user permissions at any time.)

IAM roles are the preferred method for interacting with AWS services. As a best practice, IAM roles are ideal for situations in which access to services or resources needs to be granted temporarily, rather than long term.

Consider this example of how IAM roles could be used in the coffee shop.

<click> First, the owner gives the employee permissions to switch to a role for each workstation in the coffee shop.

<click> The employee begins their day by assuming the “Cashier” role. This grants them access to the cash register system.

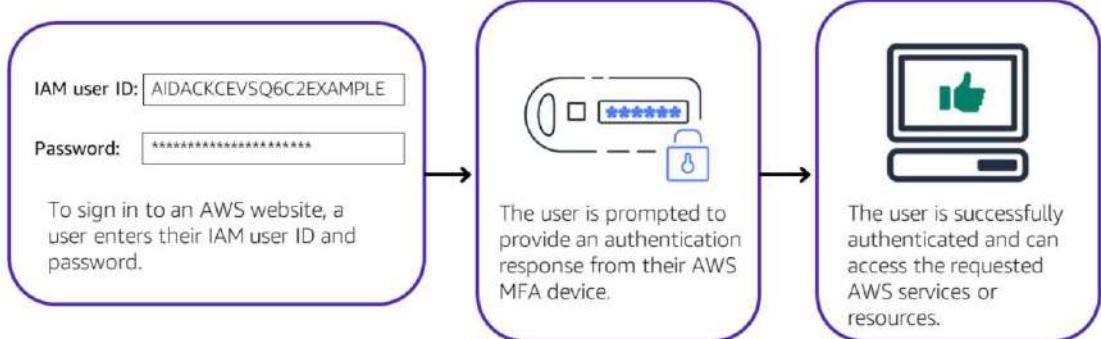
<click> Later in the day, the employee needs to update the inventory system. They assume the “Inventory” role. This grants the employee access to the inventory system and also revokes their access to the cash register system.

The final aspect of IAM that we will examine is **multi-factor authentication**.

Multi-factor authentication



Multi-factor authentication provides an extra layer of protection for your AWS account.



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

222

Have you ever logged into a website that required you to provide multiple pieces of information to verify your identity? You might have needed to provide your password and then a second form of authentication, such as a random code sent to your phone. This is an example of multi-factor authentication.

In IAM, **multi-factor authentication (MFA)** provides an extra layer of security for your AWS account.

<click> First, when a user signs into an AWS website, they enter their IAM user ID and password.

<click> Next, the user is prompted for an authentication response from their AWS MFA device. This device could be a hardware security key, a hardware device, or an MFA application on a device such as a smartphone.

<click> When the user has been successfully authenticated, they are able to access the requested AWS services or resources.

MFA can be enabled for the root user and IAM users. As a best practice, you should

enable MFA for the root user and all IAM users in your account, since this will help to keep your AWS account safe from unauthorized access.

AWS Organizations

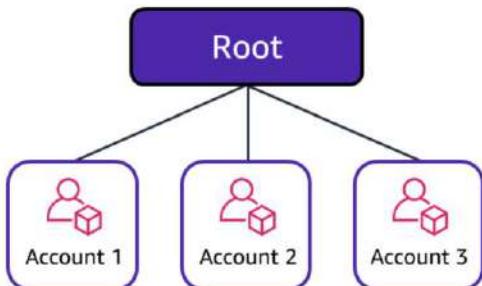
© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



In the previous section, you learned several ways to use AWS Identity and Access Management to create a separation of duties in your AWS account.

Suppose that your company has multiple AWS accounts. You can use **AWS Organizations** to consolidate and manage multiple AWS accounts in a central location.

- AWS Organizations helps customers consolidate and manage multiple AWS accounts in a central location.
- Use **service control policies (SCPs)** to centrally control permissions for the accounts in your organization.



AWS Organizations helps you consolidate and manage multiple AWS accounts within a central location.

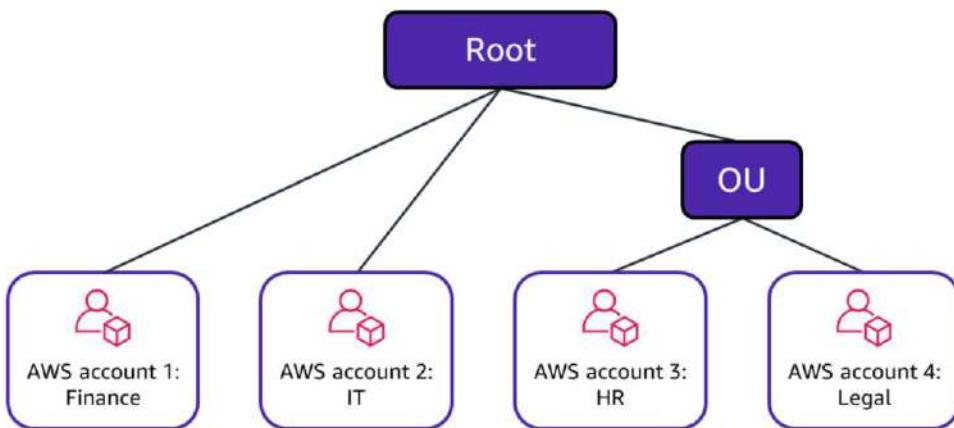
When you create an organization, AWS Organizations automatically creates a **root**, which is the parent container for all the accounts in your organization.

In AWS Organizations, you can centrally control permissions for the accounts in your organization by using **service control policies (SCPs)**. SCPs help you place restrictions on the AWS services, resources, and individual API actions that the users and roles in each account can access.

You can also apply SCPs to the root. For example, you might apply an SCP that requires that multi-factor authentication (MFA) is enabled before an IAM user or role can perform specific actions, such as stopping or terminating an Amazon EC2 instance.

(**Note:** Consolidated billing is another feature of AWS Organizations. You will learn about consolidated billing in a later module.)

Example: Organizational units



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

225

In AWS Organizations, you can group accounts into **organizational units (OUs)** to make it easier to manage accounts with similar business or security requirements. When you apply a policy to an OU, all the accounts in the OU automatically inherit the permissions specified in the policy.

By organizing separate accounts into OUs, you can more easily isolate workloads or applications that have specific security requirements. For instance, if your company has accounts that can access only the AWS services that meet certain regulatory requirements, you can put these accounts into one OU. Then, you can attach a policy to the OU that blocks access to all other AWS services that do not meet the regulatory requirements.

Imagine that your company has separate AWS accounts for the finance, information technology (IT), human resources (HR), and legal departments. You decide to consolidate these accounts into a single organization so that you can administer them from a central location. When you create the organization, this establishes the root.

In designing your organization, you consider the business, security, and regulatory needs of each department. You use this information to decide which departments

group together in OUs.

<click> The finance and IT departments have requirements that do not overlap with those of any other department. You bring these accounts into your organization to take advantage of benefits such as consolidated billing, but you do not place them into any OUs.

<click> The HR and legal departments need to access the same AWS services and resources, so you place them into an OU together. Placing them into an OU allows you to attach policies that apply to both the HR and legal departments' AWS accounts.

Even though you have placed these accounts into OUs, you can continue to provide access for users, groups, and roles through IAM.

By grouping your accounts into OUs, you can more easily give them access to the services and resources that they need. You also prevent them from accessing any services or resources that they do not need.

Knowledge check



A customer is configuring service control policies (SCPs) in AWS Organizations. Which identities and resources can SCPs be applied to? (Select TWO.)

- A. IAM users
- B. IAM groups
- C. An individual member account
- D. IAM roles
- E. An organizational unit (OU)

226.

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

You are configuring service control policies (SCPs) in AWS Organizations. Which identities and resources can SCPs be applied to? (Select TWO.)

- A. IAM users
- B. IAM groups
- C. An individual member account
- D. IAM roles
- E. An organizational unit (OU)

Knowledge check



227

A customer is configuring service control policies (SCPs) in AWS Organizations. Which identities and resources can SCPs be applied to? (Select TWO.)

- A. IAM users
- B. IAM groups
- C. An individual member account (correct)
- D. IAM roles
- E. An organizational unit (OU) (correct)

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response options are:

- C. An individual member account
- E. An organizational unit (OU)

In AWS Organizations, you can apply service control policies (SCPs) to the organization root, an individual member account, or an OU. An SCP affects all IAM users, groups, and roles within an account, including the AWS account root user.

You can apply IAM policies to IAM users, groups, or roles. You cannot apply an IAM policy to the AWS account root user.

Compliance

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



The final section of this module focuses on AWS compliance resources.

AWS Artifact



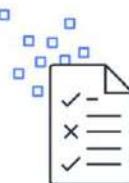
AWS Artifact provides on-demand access to security and compliance reports and select online agreements.



Access AWS compliance reports on demand



Review, accept, and manage agreements with AWS



Access compliance reports from third-party auditors

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

229

Depending on your company's industry, you might need to uphold specific standards. An audit or inspection will ensure that the company has met those standards.

AWS Artifact is a service that provides on-demand access to AWS security and compliance reports and select online agreements. AWS Artifact consists of two main sections: AWS Artifact Agreements and AWS Artifact Reports.

Suppose that your company needs to sign an agreement with AWS regarding your use of certain types of information throughout AWS services. You can do this through **AWS Artifact Agreements**.

In AWS Artifact Agreements, you can review, accept, and manage agreements for an individual account and for all your accounts in AWS Organizations. Different types of agreements are offered to address the needs of customers who are subject to specific regulations, such as the Health Insurance Portability and Accountability Act (HIPAA).

Next, suppose that a member of your company's development team is building an application and needs more information about their responsibility for complying with

certain regulatory standards. You can advise them to access this information in **AWS Artifact Reports**.

AWS Artifact Reports provide compliance reports from third-party auditors. These auditors have tested and verified that AWS is compliant with a variety of global, regional, and industry-specific security standards and regulations. AWS Artifact Reports remains up to date with the latest reports released. You can provide the AWS audit artifacts to your auditors or regulators as evidence of AWS security controls.

Assurance programs

aws training and certification



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

230

These are some of the compliance reports and regulations that you can find in AWS Artifact. Each report includes a description of its contents and the reporting period for which the document is valid.

Another resource to explore is the **Customer Compliance Center**.

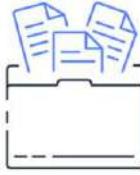
Customer Compliance Center



The **Customer Compliance Center** contains resources to help you learn more about AWS compliance.



Discover compliance stories from companies in regulated industries



Access compliance technical papers and documentation



Complete the auditor learning path

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

231

The **Customer Compliance Center** contains resources to help you learn more about AWS compliance.

In the Customer Compliance Center, you can read customer compliance stories to discover how companies in regulated industries have solved various compliance, governance, and audit challenges.

You can also access compliance whitepapers and documentation on topics such as:

- AWS answers to key compliance questions
- An overview of AWS risk and compliance
- An auditing security checklist

Additionally, the Customer Compliance Center includes an auditor learning path. This learning path is designed for individuals in auditing, compliance, and legal roles who want to learn more about how their internal operations can demonstrate compliance using the AWS Cloud.

Knowledge check



232

Which tasks can you complete in AWS Artifact? (Select TWO.)

- A. Access AWS compliance reports on-demand
- B. Consolidate and manage multiple AWS accounts in a central location
- C. Create users to allow people and applications to interact with AWS services and resources
- D. Set permissions for accounts by configuring service control policies
- E. Review, accept, and manage agreements with AWS

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which tasks can you complete in AWS Artifact? (Select TWO.)

- A. Access AWS compliance reports on-demand.
- B. Consolidate and manage multiple AWS accounts within a central location.
- C. Create users to allow people and applications to interact with AWS services and resources.
- D. Set permissions for accounts by configuring service control policies (SCPs).
- E. Review, accept, and manage agreements with AWS.

Knowledge check



235.



Which tasks can you complete in AWS Artifact? (Select TWO.)

- A. Access AWS compliance reports on-demand **(correct)**
- B. Consolidate and manage multiple AWS accounts in a central location
- C. Create users to allow people and applications to interact with AWS services and resources
- D. Set permissions for accounts by configuring service control policies
- E. Review, accept, and manage agreements with AWS **(correct)**

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response options are:

- A: Access AWS compliance reports on-demand.
- E: Review, accept, and manage agreements with AWS.

The other response options are incorrect because:

- B. Consolidate and manage multiple AWS accounts within a central location- This task can be completed in *AWS Organizations*.
- C. Create users to allow people and applications to interact with AWS services and resources. This task can be completed in *AWS Identity and Access Management (IAM)*.
- D. Set permissions for accounts by configuring service control policies (SCPs)- This task can be completed in *AWS Organizations*.

Application security

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



Throughout this course, you have learned about a wide variety of services and resources that you can use to develop and deploy applications. How can you keep these applications secure? The next aspect of security that you will examine is application security.

This section begins with **AWS Web Application Firewall**, a service that provides network security capabilities.

AWS WAF



Request from a customer

I would like to access the application.

You are coming from an IP address that is NOT blocked. You may enter!



Malicious request from a hacker

I would like to access the application.

You are coming from an IP address that IS blocked. You cannot enter.



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

235

AWS WAF is a web application firewall that lets you monitor network requests that come into your web applications.

AWS WAF works together with Amazon CloudFront and an Application Load Balancer. Recall the network access control lists that you learned about in an earlier module. AWS WAF works in a similar way to block or allow traffic. However, it does this by using a **web access control list (ACL)** to protect your AWS resources.

Here's an example of how you can use AWS WAF to allow and block specific requests.

Suppose that your application has been receiving malicious network requests from several IP addresses. You want to prevent these requests from continuing to access your application, but you also want to ensure that legitimate users can still access it. You configure the web ACL to allow all requests except those from the IP addresses that you have specified.

When a request comes into AWS WAF, it checks against the list of rules that you have configured in the web ACL. If a request did not come from one of the blocked IP addresses, it allows access to the application.

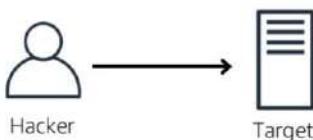
<click> However, if a request came from one of the blocked IP addresses that you have specified in the web ACL, it is denied access.

Two types of application attacks that you might need to mitigate are denial of service and distributed denial of service attacks.

DoS and DDoS attacks

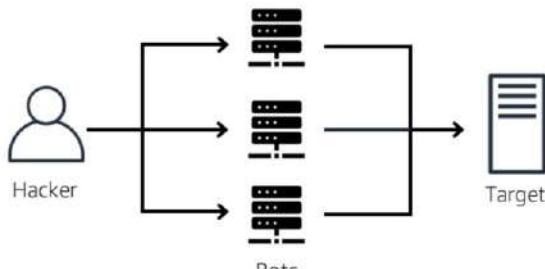


Denial of service attack



The attack originates from a **single** source.

Distributed denial of service attack



The attack originates from **multiple** sources.

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

236

Customers can call the coffee shop to place their orders. After answering each call, a cashier takes the order and gives it to the barista.

However, suppose that a prankster is calling in multiple times to place orders but is never picking up their drinks. This causes the cashier to be unavailable to take other customers' calls. The coffee shop can attempt to stop the false requests by blocking the phone number that the prankster is using.

In this scenario, the prankster's actions are similar to a **denial of service attack**.

A **denial of service (DoS) attack** is a deliberate attempt to make a website or application unavailable to users. For example, an attacker might flood a website or application with excessive network traffic until the targeted website or application becomes overloaded and is no longer able to respond. If the website or application becomes unavailable, this denies service to users who are trying to make legitimate requests.

Now, suppose that the prankster has enlisted the help of friends.

The prankster and their friends repeatedly call the coffee shop with requests to place orders, even though they do not intend to pick them up. These requests are coming in from different phone numbers, and it's impossible for the coffee shop to block them all. Additionally, the influx of calls has made it increasingly difficult for customers to be able to get their calls through. This is similar to a **distributed denial of service attack**.

<click> In a **distributed denial of service (DDoS) attack**, multiple sources are used to start an attack that aims to make a website or application unavailable. This can come from a group of attackers, or even a single attacker. The single attacker can use multiple infected computers (also known as "bots") to send excessive traffic to a website or application.

To help minimize the effect of DoS and DDoS attacks on your applications, you can use **AWS Shield**.

AWS Shield



AWS Shield provides protection against distributed denial of service (DDoS) attacks.



Protect applications against DDoS attacks



Integrate AWS Shield Advanced with other AWS services



Write custom web ACL rules with AWS WAF to mitigate complex DDoS attacks

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

237

AWS Shield is a service that protects applications against DDoS attacks. AWS Shield provides two levels of protection: Standard and Advanced.

AWS Shield Standard automatically protects all AWS customers at no cost. It protects your AWS resources from the most common, frequently occurring types of DDoS attacks. As network traffic comes into your applications, AWS Shield Standard uses a variety of analysis techniques to detect malicious traffic in real time and automatically mitigates it.

AWS Shield Advanced is a paid service that provides detailed attack diagnostics and the ability to detect and mitigate sophisticated DDoS attacks. It also integrates with other services such as Amazon CloudFront, Amazon Route 53, and Elastic Load Balancing.

Additionally, you can integrate AWS Shield with AWS WAF by writing custom rules to mitigate complex DDoS attacks.

Next, you will explore Amazon Inspector.

Amazon Inspector



Amazon Inspector allows you to perform automated security assessments on your applications.



Automatically conduct application security assessments



Identify security vulnerabilities and deviations from best practices



Receive recommendations for how to fix security issues

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

238

Suppose that the developers at the coffee shop are developing and testing a new ordering application. They want to make sure that they are designing the application in accordance with security best practices. However, they have several other applications to develop, so they cannot spend much time conducting manual assessments. To perform automated security assessments, they decide to use **Amazon Inspector**.

Amazon Inspector helps to improve the security and compliance of applications by running automated security assessments. It checks applications for security vulnerabilities and deviations from security best practices, such as open access to Amazon EC2 instances and installations of vulnerable software versions.

After Amazon Inspector has performed an assessment, it provides you with a list of security findings. The list prioritizes by severity level, including a detailed description of each security issue and a recommendation for how to fix it. However, AWS does not guarantee that following the provided recommendations resolves every potential security issue. Under the shared responsibility model, customers are responsible for the security of their applications, processes, and tools that run on AWS services.

Additional security services

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



The final section of this module examines two additional security services: AWS Key Management Service and Amazon GuardDuty.

Throughout this module, you explored the shared responsibility model, IAM, organizational security, and application security. Another aspect of security is data encryption. This can include the data in resources such as Amazon S3 buckets and Amazon RDS databases. When your data is being stored or sent, how can you ensure that it remains secure from unauthorized access?

AWS Key Management Service offers encryption capabilities, as you will see in an next example from the coffee shop.

- AWS Key Management Service (AWS KMS) helps customers perform encryption operations through the use of cryptographic keys.
- You can choose the specific levels of access control that you need for your keys.



AWS KMS

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

240

The coffee shop has many items, such as coffee machines, pastries, money in the cash registers, and so on. You can think of these items as data. The coffee shop owners want to ensure that all of these items are secure, whether they're sitting in the storage room or being transported between shop locations.

In the same way, you must ensure that your applications' data is secure while in storage (**encryption at rest**) and while it is transmitted, known as **encryption in transit**.

AWS Key Management Service (AWS KMS) allows you to perform encryption operations through the use of **cryptographic keys**. A cryptographic key is a random string of digits used for locking (encrypting) and unlocking (decrypting) data. You can use AWS KMS to create, manage, and use cryptographic keys. You can also control the use of keys across a wide range of services and in your applications.

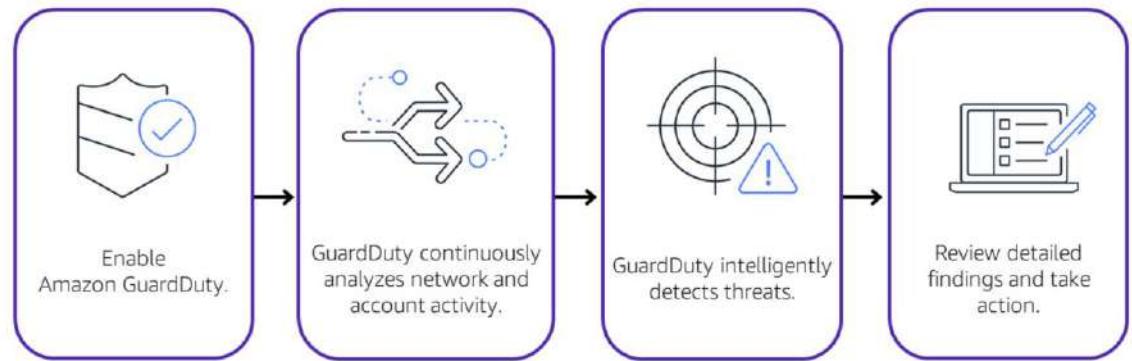
With AWS KMS, you can choose the specific levels of access control that you need for your keys. For example, you can specify which IAM users and roles are able to manage keys. Alternatively, you can temporarily disable keys so that they are no longer in use by anyone. Your keys never leave AWS KMS, and you are always in

control of them.

Amazon GuardDuty



Amazon GuardDuty provides intelligent threat detection for AWS products and services.



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

241

Amazon GuardDuty is a service that provides intelligent threat detection for your AWS infrastructure and resources. It identifies threats by continuously monitoring the network activity and account behavior within your AWS environment.

After you enable GuardDuty for your AWS account, GuardDuty begins monitoring your network and account activity. You do not have to deploy or manage any additional security software. GuardDuty then continuously analyzes data from multiple AWS sources, including VPC Flow Logs and DNS logs.

If GuardDuty detects any threats, you can review detailed findings about them from the AWS Management Console. Findings include recommended steps for remediation. You can also configure AWS Lambda functions to take remediation steps automatically in response to GuardDuty security findings.

Module 6

Knowledge check

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



Knowledge check question 1



245

Which statement describes an IAM policy?

- A. An authentication process that provides an extra layer of protection for your AWS account
- B. A document that grants or denies permissions to AWS services and resources
- C. An identity that you can assume to gain temporary access to permissions
- D. The identity that is established when you first create an AWS account

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which statement describes an IAM policy?

- A. An authentication process that provides an extra layer of protection for your AWS account
- B. A document that grants or denies permissions to AWS services and resources
- C. An identity that you can assume to gain temporary access to permissions
- D. The identity that is established when you first create an AWS account

Knowledge check answer 1



244

Which statement describes an IAM policy?

- A. An authentication process that provides an extra layer of protection for your AWS account
- B. A document that grants or denies permissions to AWS services and resources (correct)
- C. An identity that you can assume to gain temporary access to permissions
- D. The identity that is established when you first create an AWS account

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **B. A document that grants or denies permissions to AWS services and resources.**

IAM policies provide you with the flexibility to customize users' levels of access to resources. For instance, you can allow users to access all the Amazon S3 buckets in your AWS account or only a specific bucket.

The other response options are incorrect because:

A – *Multi-factor authentication (MFA)* is an authentication process that provides an extra layer of protection for your AWS account.

C – An *IAM role* is an identity that you can assume to gain temporary access to permissions.

D – The *root user identity* is the identity that is established when you first create an AWS account.

Knowledge check question 2



245

An employee requires temporary access to create several Amazon S3 buckets. Which option should be used for this task?

- A. AWS account root user
- B. IAM group
- C. IAM role
- D. Service control policy

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

An employee requires temporary access to create several Amazon S3 buckets. Which option should be used for this task?

- A. AWS account root user
- B. IAM group
- C. IAM role
- D. Service control policy (SCP)

Knowledge check answer 2



246.

An employee requires temporary access to create several Amazon S3 buckets. Which option should be used for this task?

- A. AWS account root user
- B. IAM group
- C. **IAM role (correct)**
- D. Service control policy

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct answer is **C: IAM role**.

An IAM role is an identity that you can assume to gain temporary access to permissions. When someone assumes an IAM role, they abandon all permissions that they had under a previous role and assume the permissions of the new role. IAM roles are ideal for situations in which access to services or resources needs to be granted temporarily instead of long-term.

The other response options are incorrect because:

- A. The AWS account root user is established when you first create an AWS account. As a best practice, do not use the root user for everyday tasks.
- B. Although you can attach IAM policies to an IAM group, this would not be the best choice for this scenario because the employee only needs to be granted temporary permissions.
- D. Service control policies (SCPs) allow you to centrally control permissions for the accounts in your organization. An SCP is not the best choice for granting temporary

permissions to an individual employee.

Knowledge check question 3



247

Which option describes the concept of least privilege?

- A. Adding an IAM user into at least one IAM group
- B. Granting only the permissions that are needed to perform specific tasks
- C. Checking a packet's permissions against an access control list
- D. Performing a denial of service attack that originates from at least one device

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which of the following descriptions best describes the concept of least privilege?

- A. Adding an IAM user into at least one IAM group
- B. Granting only the permissions that are needed to perform specific job tasks
- C. Checking a packet's permissions against an access control list
- D. Performing a denial of service attack that originates from at least one device

Knowledge check answer 3



248.

Which option describes the concept of least privilege?

- A. Adding an IAM user into at least one IAM group
- B. **Granting only the permissions that are needed to perform specific tasks (correct)**
- C. Checking a packet's permissions against an access control list
- D. Performing a denial of service attack that originates from at least one device

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **B: Granting only the permissions that are needed to perform specific job tasks.**

When you grant permissions by following the principle of least privilege, you prevent users or roles from having more permissions than needed to perform specific job tasks. For example, cashiers in the coffee shop should be given access to the cash register system. As a best practice, grant IAM users and roles a minimum set of permissions and then grant additional permissions as needed.

Knowledge check question 4



249

Which service helps protect your applications against distributed denial of service (DDoS) attacks?

- A. Amazon GuardDuty
- B. Amazon Inspector
- C. AWS Artifact
- D. AWS Shield

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which service helps protect your applications against distributed denial of service (DDoS) attacks?

- A. Amazon GuardDuty
- B. Amazon Inspector
- C. AWS Artifact
- D. AWS Shield

Knowledge check answer 4



250

Which service helps protect your applications against distributed denial of service (DDoS) attacks?

- A. Amazon GuardDuty
- B. Amazon Inspector
- C. AWS Artifact
- D. **AWS Shield (correct)**

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **D. AWS Shield**.

As network traffic comes into your applications, AWS Shield uses a variety of analysis techniques to detect potential DDoS attacks in real time and automatically mitigates them.

The other response options are incorrect because:

A – Amazon GuardDuty is a service that provides intelligent threat detection for your AWS infrastructure and resources. It identifies threats by continuously monitoring the network activity and account behavior within your AWS environment.

B – Amazon Inspector checks applications for security vulnerabilities and deviations from security best practices, such as open access to Amazon EC2 instances and installations of vulnerable software versions.

C – AWS Artifact is a service that provides on-demand access to AWS security and compliance reports and select online agreements.

Knowledge check question 5



251

Which task can AWS Key Management Service (AWS KMS) perform?

- A. Configure multi-factor authentication (MFA)
- B. Update the AWS account root user password
- C. Create cryptographic keys
- D. Assign permissions to users and groups

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which task can AWS Key Management Service (AWS KMS) perform?

- A. Configure multi-factor authentication (MFA).
- B. Update the AWS account root user password.
- C. Create cryptographic keys.
- D. Assign permissions to users and groups.

Knowledge check answer 5



252

Which task can AWS Key Management Service (AWS KMS) perform?

- A. Configure multi-factor authentication (MFA)
- B. Update the AWS account root user password
- C. **Create cryptographic keys (correct)**
- D. Assign permissions to users and groups

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **C. Create cryptographic keys.**

AWS KMS allows you to perform encryption operations through the use of cryptographic keys. A cryptographic key is a random string of digits used for locking (encrypting) and unlocking (decrypting) data. You can use AWS KMS to create, manage, and use cryptographic keys. You can also control the use of keys across a wide range of services and in your applications.

The other response options are incorrect because:

A – You can configure multi-factor authentication (MFA) in *AWS Identity and Access Management (IAM)*.

B – You can update the AWS account root user password in *the AWS Management Console*.

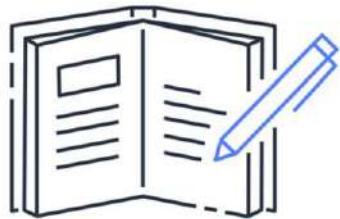
D – You can assign permissions to users and groups in *AWS Identity and Access Management (IAM)*.

Module 6 summary



In this module, you learned about:

- Shared responsibility model
- AWS Identity and Access Management features
- Methods of managing multiple accounts in AWS Organizations
- AWS services for application security and encryption
- AWS compliance resources



In this module, you learned about the AWS responsibility model, which consists of customers' responsibilities ("security **in** the cloud") and AWS responsibilities ("security **of** the cloud").

You learned about features of AWS Identity and Access Management, including:

- AWS account root user
- IAM users
- IAM policies
- IAM groups
- IAM roles
- Multi-factor authentication

In the section on AWS Organizations, you learned how to use organizational units and SCPs to centrally manage multiple AWS accounts.

You also explored several AWS services for application security and encryption:

- AWS Web Application Firewall

- AWS Shield
- Amazon GuardDuty
- Amazon Inspector
- AWS Key Management Services

Finally, you learned about AWS compliance resources: AWS Artifact and the Customer Compliance Center.

The next module explores AWS services for monitoring and analytics.

Module 7

Monitoring and Analytics



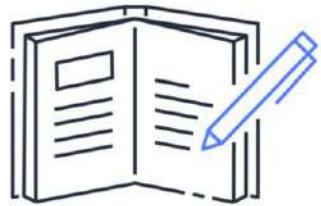
In this module, you will learn about three services for monitoring and analyzing your AWS environment: Amazon CloudWatch, AWS CloudTrail, and AWS Trusted Advisor.

Module 7 objectives



In this module, you will learn how to:

- Summarize approaches to monitoring in AWS
- Describe Amazon CloudWatch benefits
- Describe AWS CloudTrail benefits
- Describe AWS Trusted Advisor benefits



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

355

In this module, you will learn how to:

- Summarize approaches to monitoring in AWS
- Describe Amazon CloudWatch benefits
- Describe AWS CloudTrail benefits
- Describe AWS Trusted Advisor benefits

Amazon CloudWatch

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

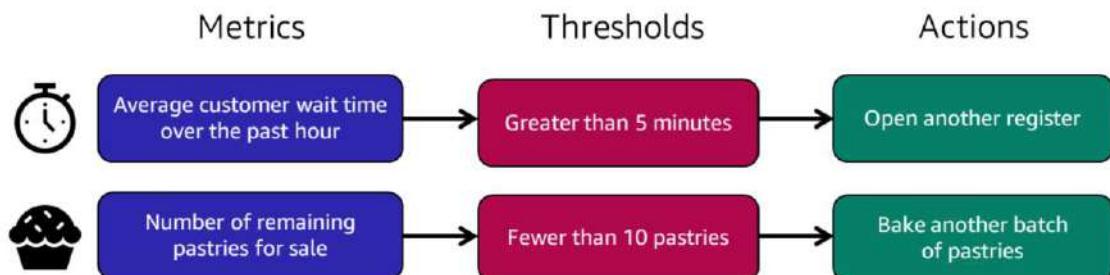


Throughout this course, you have explored topics such as creating AWS resources, delivering content to your customers, and keeping your environment secure.

This module focuses on the topics of monitoring and analytics. Monitoring and analyzing your AWS infrastructure can help you optimize usage, identify actions that require an immediate response, and refine business processes.

The first monitoring service that you will examine is Amazon CloudWatch. The next section begins with an example from the coffee shop.

Coffee shop metrics



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

257

Whenever the owner is in the coffee shop, they monitor how the business is operating throughout the day. For example, they calculate the average customer wait time over the past hour and identify the number of remaining pastries for sale. These are examples of **metrics**. You can think of a metric as a variable that is monitored for a resource.

<click> The owner monitors these metrics and notices if any of them happen to exceed or fall below specific thresholds. If any areas require immediate action, the owner can respond to them right away.

For instance, whenever the owner notices that the average customer wait time exceeds 5 minutes, they open another register. Whenever the owner notices that only 10 pastries are remaining, they bake another batch.

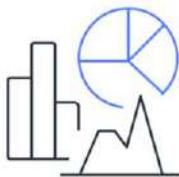
However, going back and forth between workstations to observe them one at a time is not feasible for the owner. The owner needs a system that they can use to monitor multiple parts of the coffee shop at once, receive a notification if any metrics exceed or fall below specific thresholds, and automatically respond to performance or usage issues.

The next section explores how you can use Amazon CloudWatch to monitor your AWS resources and configure automatic actions for them.

Amazon CloudWatch



Monitor your AWS and on-premises infrastructure and resources in real time



Access all of your metrics from a single location



Configure automatic alerts and actions in response to metrics

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

258

Amazon CloudWatch is a web service that allows you to monitor and manage various metrics, and configure alarm actions based on data from those metrics.

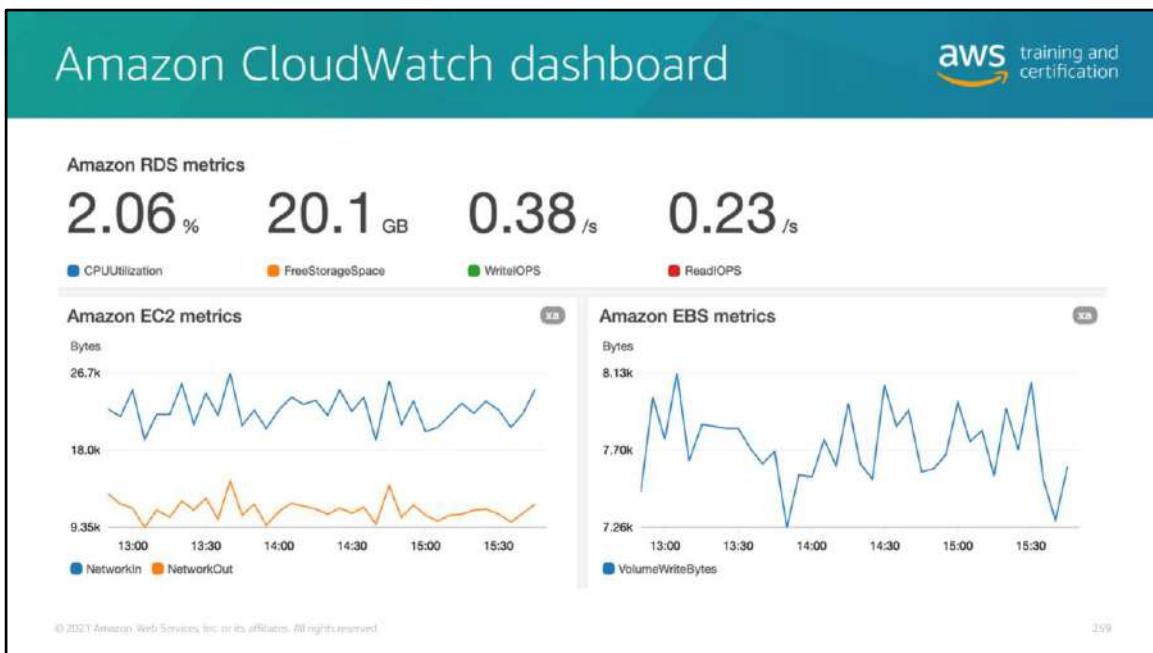
CloudWatch uses **metrics** to represent the data points for your resources. AWS services send metrics to CloudWatch. CloudWatch uses the metrics to create graphs automatically that show how performance has changed over time.

With CloudWatch, you can create **alarms** that automatically perform actions if the value of a metric goes above or below a predefined threshold.

For example, suppose that your company's developers use Amazon Elastic Compute Cloud (Amazon EC2) instances for application development or testing purposes. If the developers occasionally forget to stop the instances, the instances will continue to run and incur charges.

In this scenario, you could create a CloudWatch alarm that automatically stops an Amazon EC2 instance when the CPU usage percentage has remained below a certain threshold for a specified period. When configuring the alarm, you can specify to receive a notification whenever the alarm is triggered.

The next section explores an example of how data is presented in a CloudWatch dashboard.



Consider this example. Suppose that the coffee shop has an application that uses Amazon Relational Database Service (Amazon RDS) instances, Amazon EC2 instances, and Amazon Elastic Block Store (Amazon EBS) volumes.

The coffee shop owner uses the CloudWatch **dashboard** feature to access all the metrics for their resources from a single location. For example, they can use a CloudWatch dashboard to monitor the CPU usage of an Amazon EC2 instance, the total number of requests made to an Amazon Simple Storage Service (Amazon S3) bucket, and more. They can even customize separate dashboards for different business purposes, applications, or resources.

AWS CloudTrail

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



In addition to monitoring the performance of AWS resources, you might also want to track all the user actions and API requests that occur throughout your AWS environment.

The service that provides this functionality is **AWS CloudTrail**. To learn about CloudTrail, the next section explores another example from the coffee shop.

Coffee shop events



3 days ago

2 days ago

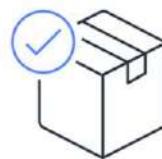
Today



The cashiers process a large number of transactions.



To avoid running out of supplies, the inventory specialist places an extra order.



A shipment of coffee beans is delivered to the coffee shop.

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

261

One day at the coffee shop, the owner receives an unexpected delivery of coffee beans. The regular shipment isn't scheduled to arrive for another week, so the owner is unsure why this shipment of coffee beans has arrived now.

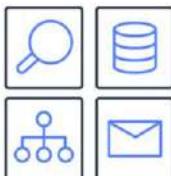
<click> The owner retraces events that occurred over the past few days. They check the inventory system and discover that the inventory specialist placed an order for coffee beans two days ago.

<click> Next, the owner reviews the transaction logs from the point of sale system. They discover that due to an unexpected increase in business three days ago, the shop was forecasted to run out of coffee beans before its next shipment. This is why the inventory specialist needed to place an additional order.

Reviewing the coffee shop's event history can help the owner answer questions about which actions were taken, when they occurred, and which users or resources were involved.

To review activities that occur throughout your AWS environment, you can use AWS CloudTrail.

AWS CloudTrail



Track user activities and API requests throughout your AWS infrastructure



Filter logs generated by API calls to assist with operational analysis and troubleshooting



Automatically detect unusual account activity

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

262

AWS CloudTrail records API calls for your account. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, and more. You can think of CloudTrail as a “trail” of breadcrumbs (or a log of actions) that someone left behind them.

Recall that you can use API calls to provision, manage, and configure your AWS resources. With CloudTrail, you can view a complete history of user activity and API calls for your applications and resources.

Events are typically updated in CloudTrail within 15 minutes after an API call. You can filter events by specifying the time and date that an API call occurred, the user who requested the action, the type of resource involved in the API call, and more.

In CloudTrail, you can also enable **CloudTrail Insights**. This optional feature allows CloudTrail to automatically detect unusual API activities in your AWS account.

For example, CloudTrail Insights might detect that a higher number of Amazon EC2 instances than usual have recently launched in your account. You can then review the full event details to determine which actions you must take.

Next, you will review an example of how the coffee shop might use AWS CloudTrail.

AWS CloudTrail event



What happened?

- New IAM user (Mary) created



Who made the request?

- IAM user John



When did this occur?

- January 1, 2021 at 9:00 AM



How was the request made?

- Through the AWS Management Console



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

263

Suppose that the coffee shop owner is browsing through the AWS Identity and Access Management (IAM) section of the AWS Management Console. They discover that a new IAM user named Mary was created, but they do not know who, when, or which method created the user.

To answer these questions, the owner navigates to AWS CloudTrail.

In the CloudTrail Event History section, the owner applies a filter to display only the events for the “CreateUser” API action in IAM. The owner locates the event for the API call that created an IAM user for Mary. This event record provides complete details about what occurred:

On January 1, 2021 at 9:00 AM, IAM user John created a new IAM user (Mary) through the AWS Management Console.

Knowledge check question



264

Which tasks can you perform using AWS CloudTrail? (Select TWO.)

- A. Monitor your AWS infrastructure and resources in real time
- B. Track user activities and API requests throughout your AWS infrastructure
- C. View metrics and graphs to monitor the performance of resources
- D. Filter logs to assist with operational analysis and troubleshooting
- E. Configure automatic actions and alerts in response to metrics

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which tasks can you perform using AWS CloudTrail? (Select TWO.)

- A. Monitor your AWS infrastructure and resources in real time
- B. Track user activities and API requests throughout your AWS infrastructure
- C. View metrics and graphs to monitor the performance of resources
- D. Filter logs to assist with operational analysis and troubleshooting
- E. Configure automatic actions and alerts in response to metrics

Knowledge check answer



265

Which tasks can you perform using AWS CloudTrail? (Select TWO.)

- A. Monitor your AWS infrastructure and resources in real time
- B. **Track user activities and API requests throughout your AWS infrastructure (correct)**
- C. View metrics and graphs to monitor the performance of resources
- D. **Filter logs to assist with operational analysis and troubleshooting (correct)**
- E. Configure automatic actions and alerts in response to metrics

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The two correct response options are:

- B. Track user activities and API requests throughout your AWS infrastructure**
- D. Filter logs to assist with operational analysis and troubleshooting**

The other response options are tasks that you can perform in Amazon CloudWatch.

AWS Trusted Advisor

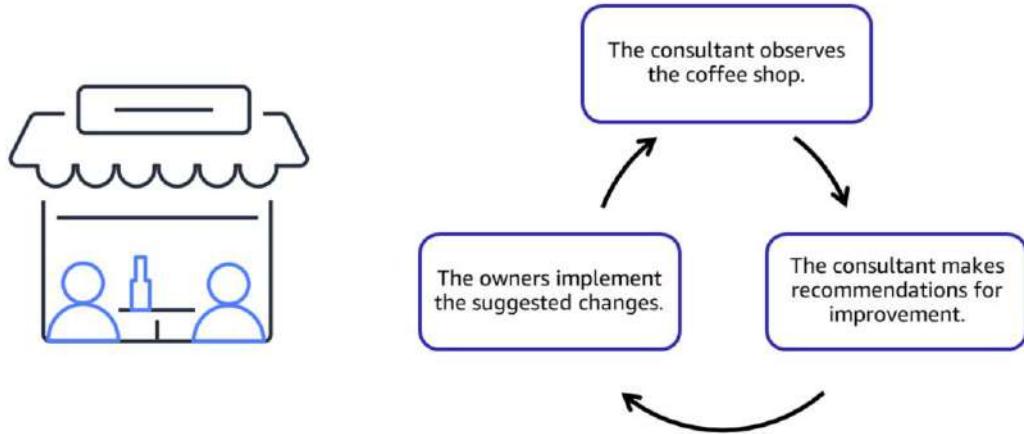
© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



Next, you will examine how to use data and insights about your AWS resources to identify potential areas of improvement.

A service that provides recommendations for improving your AWS environment is **AWS Trusted Advisor**. The next section uses a coffee shop example to introduce you to Trusted Advisor.

Coffee shop improvements



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

267

Now that the coffee shop has been in business for a while, the owners want to improve their operations. They enlist the help of a coffee shop consultant.

The consultant observes the coffee shop's current business practices, such as order-taking processes, use of supplies, methods for securing digital records, and so on. The consultant compares their observations to established best practices for running a coffee shop.

As the consultant completes their observations, they provide the owners with a summary of their findings and their recommended areas of improvement. This allows the owners to more easily begin making specific changes throughout the shop. Later, the owners can invite the consultant to come back to conduct additional observations and determine which other improvements might benefit the coffee shop.

To receive real-time guidance for how to make improvements throughout your AWS environment, you can use AWS Trusted Advisor.

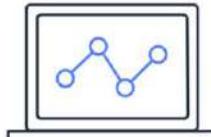
AWS Trusted Advisor



Receive real-time guidance for improving your AWS environment



Compare your infrastructure to AWS best practices in five categories



Evaluate and implement guidance at all stages of deployment

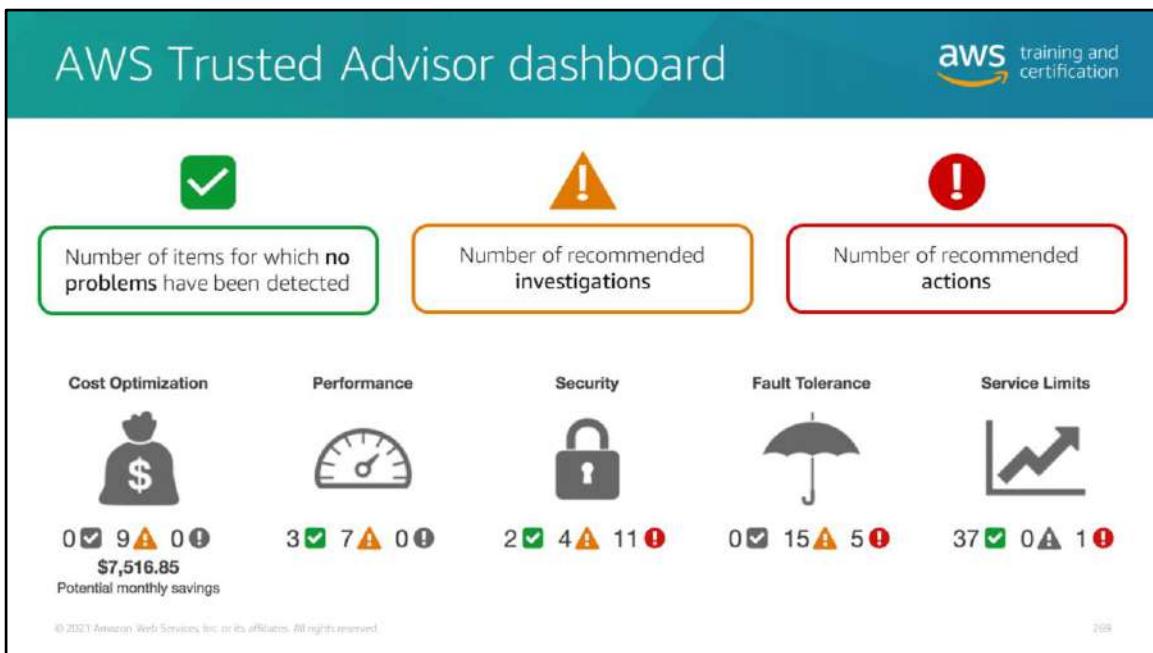
© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

268

AWS Trusted Advisor is a web service that inspects your AWS environment and provides real-time recommendations in accordance with AWS best practices.

Trusted Advisor compares its findings to AWS best practices in five categories: cost optimization, performance, security, fault tolerance, and service limits. For the checks in each category, Trusted Advisor offers a list of recommended actions and additional resources to learn more about AWS best practices.

The guidance provided by AWS Trusted Advisor can benefit your company at all stages of deployment. For example, you can use AWS Trusted Advisor to assist you while you are creating new workflows and developing new applications. Or, you can use it while you are making ongoing improvements to existing applications and resources.



When you access the Trusted Advisor dashboard in the AWS Management Console, you can review completed checks for cost optimization, performance, security, fault tolerance, and service limits, as shown in this example.

For each category:

- The green check indicates the number of items for which it detected **no problems**.
- The orange triangle represents the number of recommended **investigations**.
- The red circle represents the number of recommended **actions**.

Here are a few examples of what these alerts might indicate for Trusted Advisor's checks in Amazon S3:

- A yellow investigation alert might occur if a bucket's access control list allows any authenticated AWS user to view the objects in the bucket.
- A red action alert might occur if a bucket's access control list allows any authenticated AWS user to upload files to the bucket or delete existing objects.

Although both of these alerts should be remediated, the red alert indicates a greater

sense of urgency for action that needs to be taken.

Module 7

Knowledge check

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



Knowledge check question 1



271

Which actions can you perform using Amazon CloudWatch? (Select TWO.)

- A. Monitor your resources' usage and performance
- B. Receive real-time guidance for improving your AWS environment
- C. Compare your infrastructure to AWS best practices in five categories
- D. Access metrics from a single dashboard
- E. Automatically detect unusual account activity

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which actions can you perform using Amazon CloudWatch? (Select TWO.)

- A. Monitor your resources' usage and performance
- B. Receive real-time guidance for improving your AWS environment
- C. Compare your infrastructure to AWS best practices in five categories
- D. Access metrics from a single dashboard
- E. Automatically detect unusual account activity

Knowledge check answer 1



272

Which actions can you perform using Amazon CloudWatch? (Select TWO.)

- A. Monitor your resources' usage and performance (correct)
- B. Receive real-time guidance for improving your AWS environment
- C. Compare your infrastructure to AWS best practices in five categories
- D. Access metrics from a single dashboard (correct)
- E. Automatically detect unusual account activity

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The two correct response options are:

- A. Monitor your resources' usage and performance
- D. Access metrics from a single dashboard

The other response options are incorrect because:

- B. Receiving real-time recommendations for improving your AWS environment can be performed by *AWS Trusted Advisor*.
- C. Comparing your infrastructure to AWS best practices in five categories can be performed by *AWS Trusted Advisor*.
- E. Automatically detecting unusual account activity can be performed by *AWS CloudTrail*.

Knowledge check question 2



275

Which service can you use to review the security of your Amazon S3 buckets by checking for open access permissions?

- A. Amazon CloudWatch
- B. AWS CloudTrail
- C. AWS Trusted Advisor
- D. Amazon GuardDuty

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which service can you use to review the security of your Amazon S3 buckets by checking for open access permissions?

- A. Amazon CloudWatch
- B. AWS CloudTrail
- C. AWS Trusted Advisor
- D. Amazon GuardDuty

Knowledge check answer 2



274

Which service can you use to review the security of your Amazon S3 buckets by checking for open access permissions?

- A. Amazon CloudWatch
- B. AWS CloudTrail
- C. **AWS Trusted Advisor (correct)**
- D. Amazon GuardDuty

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **C. AWS Trusted Advisor**.

AWS Trusted Advisor is a web service that inspects your AWS environment and provides real-time recommendations in accordance with AWS best practices. The inspection includes security checks, such as Amazon S3 buckets with open access permissions.

The other response options are incorrect because:

- A. Amazon CloudWatch is a web service that allows you to monitor and manage various metrics for the resources that run your applications.
- B. AWS CloudTrail is a web service that allows you to review details for user activities and API calls that have occurred in your AWS environment.
- D. Amazon GuardDuty is a service that provides intelligent threat detection for your AWS environment and resources. It identifies threats by continuously monitoring the network activity and account behavior in your AWS environment.

Knowledge check question 3



275

Which categories are included in the AWS Trusted Advisor dashboard? (Select TWO.)

- A. Reliability
- B. Performance
- C. Scalability
- D. Elasticity
- E. Fault tolerance

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which categories are included in the AWS Trusted Advisor dashboard? (Select TWO.)

- A. Reliability
- B. Performance
- C. Scalability
- D. Elasticity
- E. Fault tolerance

Knowledge check answer 3



276

Which categories are included in the AWS Trusted Advisor dashboard? (Select TWO.)

- A. Reliability
- B. **Performance (correct)**
- C. Scalability
- D. Elasticity
- E. **Fault tolerance (correct)**

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The two correct response options are:

- **B. Performance**
- **E. Fault tolerance**

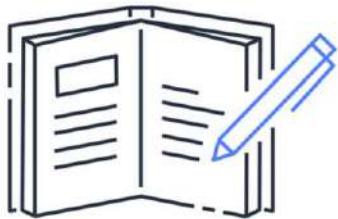
AWS Trusted Advisor continuously inspects your AWS environment and provides best practice recommendations across five categories: cost optimization, performance, security, fault tolerance, and service limits.

Module 7 summary



In this module, you learned about:

- Amazon CloudWatch
- AWS CloudTrail
- AWS Trusted Advisor



In this module, you learned about three AWS services for monitoring and analytics:

- **Amazon CloudWatch** is a service that monitors usage and performance for the resources that run your applications.
- **AWS CloudTrail** is a service that you can use to review details for user activities and API requests that occur in your AWS environment.
- **AWS Trusted Advisor** is a service that scans your infrastructure and provides real-time guidance in accordance with AWS best practices.

In the next module, you will explore AWS pricing and support.

Module 8

Pricing and Support



In this module, you will learn about AWS pricing concepts, tools, and examples. You will also explore AWS Support plans and learn about the benefits of AWS Marketplace.

Module 8 objectives



In this module, you will learn how to:

- Describe AWS pricing and support models
- Describe the AWS Free Tier
- Describe key benefits of AWS Organizations and consolidated billing
- Explain AWS Budgets benefits
- Explain AWS Cost Explorer benefits
- Explain AWS Pricing Calculator benefits
- Distinguish among the AWS Support plans
- Describe AWS Marketplace benefits

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.279

In this module, you will learn how to:

- Describe AWS pricing and support models
- Describe the AWS Free Tier
- Describe key benefits of AWS Organizations and consolidated billing
- Explain AWS Budgets benefits
- Explain AWS Cost Explorer benefits
- Explain AWS Pricing Calculator benefits
- Distinguish among the AWS Support plans
- Describe AWS Marketplace benefits

AWS pricing and support



How can I budget
and pay for AWS
services?

Where can I find
support and third-
party software?



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

200

Throughout this course, you have learned about a wide range of AWS services and resources that can help you to develop innovative solutions for your company.

At this point, you might be wondering about the pricing and support options that AWS offers for these services.

In this module, you will learn about some of the tools that you can use for AWS pricing and support. These tools can help you answer these questions and provide new opportunities for optimizing your costs while using AWS services.

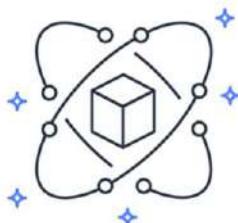
AWS pricing

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

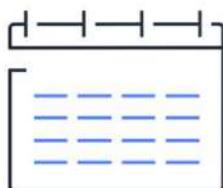


This section examines AWS pricing models, beginning with the AWS Free Tier.

AWS Free Tier categories



Always free



12 months free



Trials

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

2/2

The **AWS Free Tier** lets you begin using certain services without incurring costs for the specified period.

Three types of offers are available:

Always Free: These offers do not expire and are available to all AWS customers. For example, AWS Lambda allows 1 million free requests and up to 3.2 million seconds of compute time per month. Amazon DynamoDB allows 25 GB of free storage per month.

12 Months Free: These offers are free for 12 months following your initial sign-up date to AWS. Examples include specific amounts of Amazon S3 Standard Storage, thresholds for monthly hours of Amazon Elastic Compute Cloud (Amazon EC2) compute time, and amounts of Amazon CloudFront data transfer out.

Trials: Short-term free trial offers start from the date you activate a particular service. The length of each trial might vary by number of days or the amount of usage in the service. For example, Amazon Inspector offers a 90-day free trial. Amazon Lightsail (a service that you can use to run virtual private servers) offers 750 free hours of usage.

over a 30-day period.

For each AWS Free Tier offer, review the specific details about exactly which resource types are included.

After you use AWS services for a while, you might go beyond what is included in the Free Tier. You should know how AWS pricing works, which described next.

AWS pricing concepts



Pay as you go

Pay only for the resources that you use without provisioning capacity in advance

Pay less when you reserve

Reduce costs by reserving capacity in services such as Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Relational Database Service (Amazon RDS)

Pay less with volume-based discounts

Receive savings through volume-based discounts as your usage increases

AWS offers a range of cloud computing services with pay-as-you-go pricing.

Pay for what you use: For each service, you pay for exactly the amount of resources that you actually use, without requiring long-term contracts or complex licensing.

Pay less when you reserve: Some services offer reservation options that provide a significant discount compared to On-Demand Instance pricing. For example, suppose that your company is using Amazon EC2 instances for a workload that needs to run continuously. You might choose to run this workload on Amazon EC2 Instance Savings Plans, because the plan allows you to save up to 72% over the equivalent On-Demand Instance capacity.

Pay less with volume-based discounts: Some services offer tiered pricing, so the per-unit cost is incrementally lower with increased usage. For example, the more Amazon S3 storage space you use, the less you pay for it per GB.

The screenshot shows the AWS Pricing Calculator interface. At the top, there's a navigation bar with the AWS logo, a search bar labeled "aws pricing calculator", and links for "Feedback", "English", and "Contact Sales". Below the bar, the title "AWS Pricing Calculator" is displayed, followed by the "aws training and certification" logo. The main content area is titled "Configure Amazon EC2" with an "Info" link. It starts with "Step 1 Select service" and "Step 2 Configure Amazon EC2". A dropdown menu for "Region" is set to "US East (Ohio)". There are two estimation options: "Quick estimate" (selected) and "Advanced estimate". The "Quick estimate" section is described as providing a fast and easy route to a ballpark estimate based on minimum requirements or a specific instance search. The "Advanced estimate" section is described as choosing this option for a more detailed estimate that accounts for workload, data transfer costs, additional storage options, and either less or more common instance requirements. Below this, there's a section for "EC2 instance specifications" with an "Info" link. Under "Operating system", it says "Choose which operating system you'd like to run Amazon EC2 instances on." with a dropdown menu showing "Linux". At the bottom left, there's a copyright notice: "© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved." and at the bottom right, a page number "2/64".

The **AWS Pricing Calculator** lets you explore AWS services and create an estimate for the cost of your use cases on AWS. You can organize your AWS estimates by groups that you define. A group can reflect how your company is organized, such as provide estimates by cost center.

When you create an estimate, you can save it and generate a link to share with others.

Suppose that your company is interested in using Amazon EC2. However, you are not yet sure which AWS Region or instance type would be the most cost-efficient for your use case. In the AWS Pricing Calculator, you can enter details such as the kind of operating system you need, memory requirements, and input/output (I/O) requirements. By using the AWS Pricing Calculator, you can review an estimated comparison of different EC2 instance types across AWS Regions.

Next, you will explore three examples of pricing in AWS services.

AWS Lambda pricing



- Pay only for the compute time you use
- Pay for the number of requests for your functions
- Save by signing up for a Compute Savings Plan



AWS Lambda

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

205

For AWS Lambda, you are charged based on the number of requests for your functions and the amount of time that they run.

AWS Lambda allows 1 million free requests and up to 3.2 million seconds of compute time per month.

You can save on AWS Lambda costs by signing up for a Compute Savings Plan. A Compute Savings Plan offers lower compute costs in exchange for committing to a consistent amount of usage over a 1-year or 3-year term. This is an example of **paying less when you reserve**.

Example: AWS Lambda service charges



- Lambda		\$0.00
- US East (N. Virginia)		\$0.00
AWS Lambda Lambda-GB-Second		\$0.00
AWS Lambda - Compute Free Tier - 400,000 GB-Seconds - US East (Northern Virginia)	254.575 seconds	\$0.00
AWS Lambda Request		\$0.00
AWS Lambda - Requests Free Tier - 1,000,000 Requests - US East (Northern Virginia)	680.000 Requests	\$0.00

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

2/6

If you use AWS Lambda in multiple AWS Regions, you can view the itemized charges by Region on your bill.

In this example, all the AWS Lambda usage occurred in the Northern Virginia Region. The bill lists separate charges for the number of requests for functions and their duration.

Both the number of requests and the total duration of requests are under the thresholds in the AWS Free Tier, so the account owner does not have to pay for any AWS Lambda usage in this month.

Amazon EC2 pricing



- Pay only for the time that your On-Demand Instances run
- Reduce costs by using Spot Instances for recommended use cases
- Save by signing up for a Compute Savings Plan
- Amazon EC2 pricing:
<https://aws.amazon.com/ec2/pricing>



Amazon Elastic Compute
Cloud

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

207

With Amazon EC2, you pay for only the compute time that you use while your On-Demand Instances are running.

For some workloads, you can significantly reduce Amazon EC2 costs by using Spot Instances. For example, suppose that you are running a batch processing job that can be interrupted. Using a Spot Instance would provide up to a 90% discount over the On-Demand Instance price.

You can find additional cost savings for Amazon EC2 by considering Savings Plans and Reserved Instances.

Amazon EC2 pricing is based on the type of instances that you are running. For more information on Amazon EC2 pricing, review <https://aws.amazon.com/ec2/pricing/>.

Example: Amazon EC2 service charges



▼ Elastic Compute Cloud		\$0.00
▼ US East (N. Virginia)		\$0.00
Amazon Elastic Compute Cloud running Linux/UNIX		\$0.00
\$0.00 per Linux t2.micro instance-hour (or partial hour) under monthly free tier	106.512 Hrs	\$0.00
EBS		\$0.00
\$0.00 per GB-month of General Purpose (SSD) provisioned storage under monthly free tier	11.294 GB-Mo	\$0.00
Elastic Load Balancing - Application		\$0.00
\$0.00 per Application LoadBalancer-hour (or partial hour) under monthly free tier	268.000 Hrs	\$0.00

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

2/8

The service charges in this example include details for the following items:

- Each Amazon EC2 instance type in use
- Amount of Amazon Elastic Block Store (Amazon EBS) storage space provisioned
- Length of time Elastic Load Balancing was used

In this example, all the usage amounts are under the thresholds in the AWS Free Tier, so the account owner does not have to pay for any Amazon EC2 usage in this month.

Amazon S3 pricing



Amazon S3 pricing is based on four factors:

- Storage
- Requests and data retrievals
- Data transfer
- Management and replication



Amazon Simple Storage
Service

For Amazon S3 pricing, consider the following cost components:

- **Storage:** You pay for only the storage that you use. You are charged the rate to store objects in your Amazon S3 buckets based on your objects' sizes, storage classes, and length of storage for each object during the month.
- **Requests and data retrievals:** You pay for requests made to your Amazon S3 objects and buckets. For example, suppose that you are storing photo files in Amazon S3 buckets and hosting them on a website. Every time a visitor requests the website that includes the photo files, this counts towards requests you must pay for.
- **Data transfer:** There is no cost to transfer data between different Amazon S3 buckets or from Amazon S3 to other services in the same AWS Region. However, you pay for data that you transfer into and out of Amazon S3, with a few exceptions. Data transferred into Amazon S3 from the internet or out to Amazon CloudFront incurs no cost. In addition, data transferred out to an Amazon EC2 instance in the same AWS Region as the Amazon S3 bucket incurs no cost.

- **Management and replication:** You pay for the storage management features that you enabled on your account's Amazon S3 buckets. These features include Amazon S3 inventory, analytics, and object tagging.

Example: Amazon S3 service charges



Simple Storage Service	\$0.00
US East (N. Virginia)	\$0.00
Amazon Simple Storage Service Requests-Tier1 \$0.00 per request - PUT, COPY, POST, or LIST requests under the monthly global free tier	\$0.00
185.000 Requests	\$0.00
Amazon Simple Storage Service Requests-Tier2 \$0.00 per request - GET and all other requests under the monthly global free tier	\$0.00
923.000 Requests	\$0.00
Amazon Simple Storage Service TimedStorage-ByteHrs \$0.000 per GB - storage under the monthly global free tier	\$0.00
0.159 GB-Mo	\$0.00
US East (Ohio)	\$0.00
Amazon Simple Storage Service USE2-Requests-Tier2 \$0.00 per request - GET and all other requests under the monthly global free tier	\$0.00
4.000 Requests	\$0.00
Amazon Simple Storage Service USE2-TimedStorage-ByteHrs \$0.000 per GB - storage under the monthly global free tier	\$0.00
0.000001 GB-Mo	\$0.00

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

290

The AWS account in this example uses Amazon S3 in two Regions: Northern Virginia and Ohio. For each Region, itemized charges are based on the following factors:

- Number of requests to add or copy objects into a bucket
- Number of requests to retrieve objects from a bucket
- Amount of storage space used

All the usage for Amazon S3 in this example is under the AWS Free Tier limits, so the account owner does not have to pay for any Amazon S3 usage in this month.

Demo: Billing dashboard in the AWS Management Console

Instructor notes

This demo focuses on showing participants how to access the Billing section of the AWS Management Console. We recommend that you include the following areas:

- Searching for “Billing” in the Services menu.
- Reviewing your AWS bill, including:
 - Service costs by Region
 - Month to date spend
 - Top services being used
 - Current and forecasted amounts
 - Top Free Tier services by usage
- Accessing other billing tools, such as Cost Explorer, Budgets, and Budgets Reports.

Knowledge check question



292

The AWS Free Tier includes offers that are available to new AWS customers for a certain period of time following their AWS sign-up date. What is the duration of this period?

- A. 3 months
- B. 6 months
- C. 9 months
- D. 12 months

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The AWS Free Tier includes offers that are available to new AWS customers for a certain period of time following their AWS sign-up date. What is the duration of this period?

- A. 3 months
- B. 6 months
- C. 9 months
- D. 12 months

Knowledge check answer



293.

The AWS Free Tier includes offers that are available to new AWS customers for a certain period of time following their AWS sign-up date. What is the duration of this period?

- A. 3 months
- B. 6 months
- C. 9 months
- D. **12 months (correct)**

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **D. 12 months**.

The AWS Free Tier consists of three types of offers that allow customers to use AWS services without incurring costs: Always Free, 12 Months Free, and Trials.

For 12 months after you first sign up for an AWS account, you can use offers in the **12 Months Free** category. Examples of offers in this category include specific amounts of Amazon S3 Standard Storage, thresholds for monthly hours of Amazon EC2 compute time, and amounts of Amazon CloudFront data transfer out.

Consolidated billing

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

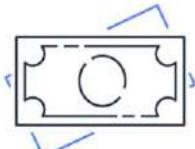


In an earlier module, you learned about AWS Organizations, a service that you can use to manage multiple AWS accounts from a central location. AWS Organizations also provides the option for **consolidated billing**.

Consolidated billing



Receive a single bill
for all the AWS
accounts in your
organization



Review itemized
charges that have been
incurred by each
account



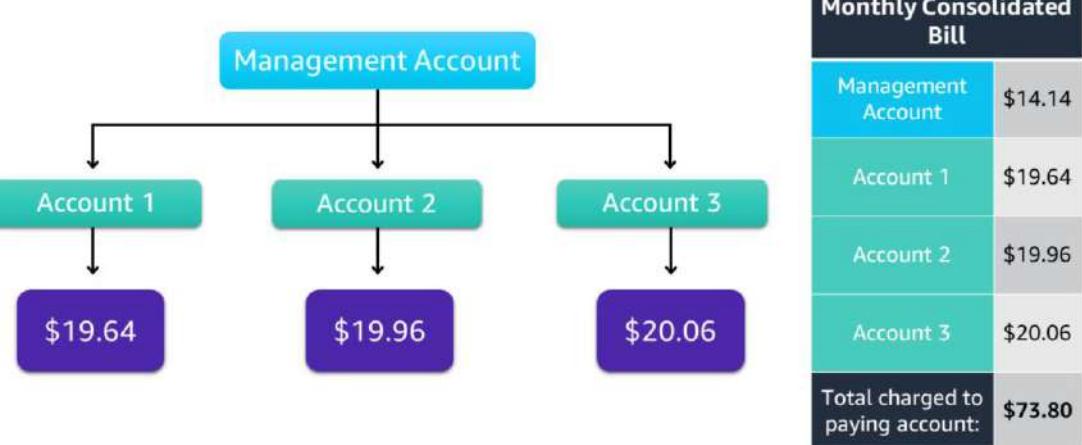
Share savings across
the accounts in your
organization

The **consolidated billing** feature of AWS Organizations allows you to receive a single bill for all AWS accounts in your organization. By consolidating, you can track the combined costs of all the linked accounts in your organization. The default maximum number of accounts allowed for an organization is four, but you can contact AWS Support to increase your quota, if needed.

On your monthly bill, you can review itemized charges incurred by each account. This provides transparency into your organization's accounts while maintaining the convenience of receiving a single monthly bill.

Another benefit of consolidated billing is the ability to share bulk discount pricing, Savings Plans, and Reserved Instances across the accounts in your organization. For instance, one account might not have enough monthly usage to qualify for discount pricing. However, when multiple accounts are combined, their aggregated usage might result in a benefit that applies across all accounts in the organization.

Example: Consolidated billing



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

296

Suppose that you are the business leader who oversees your company's AWS billing.

Your company has three AWS accounts used for separate departments. Instead of paying each location's monthly bill separately, you decide to create an organization and add the three accounts.

You manage the organization through the management account.

<click> Each month, AWS charges your management payer account for all the linked accounts in a consolidated bill. Through the management account, you can also get a detailed cost report for each linked account.

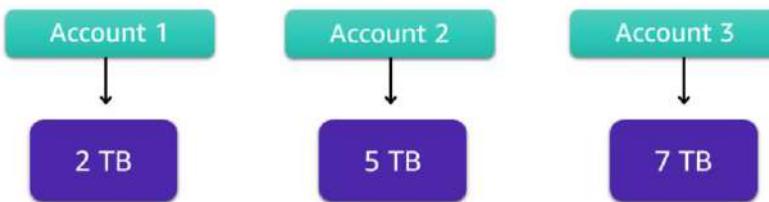
The monthly consolidated bill also includes the account usage costs incurred by the management account. This cost is not a premium charge for having a management account.

The consolidated bill shows the costs associated with any actions of the management account (such as storing files in Amazon S3 or running Amazon EC2 instances).

Fun trivia note: The dollar values on this slide correspond to significant years in Amazon's history:

- *1964 is the year in which Jeff Bezos was born.*
- *1996 is the year in which Amazon was founded.*
- *2006 is the year in which AWS was founded.*

Example: Volume pricing in Amazon S3



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

297

Consolidated billing also lets you share volume pricing discounts across accounts.

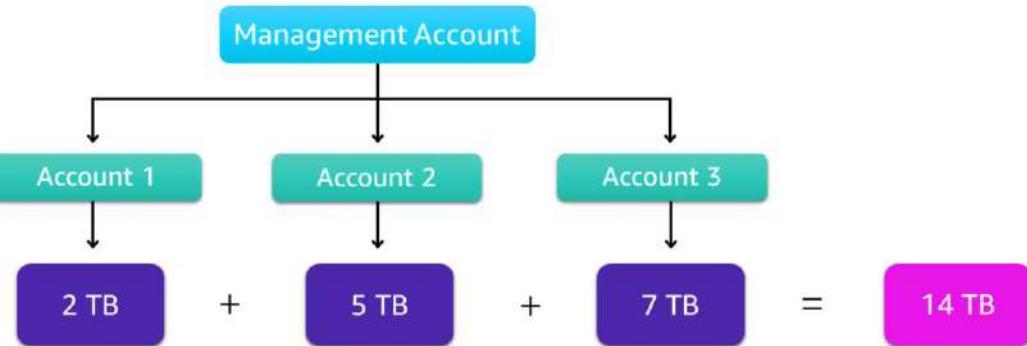
Some AWS services, such as Amazon S3, provide volume pricing discounts that give you lower prices the more that you use the service. In Amazon S3, after customers transfer 10 TB of data in a month, they pay a lower per-GB transfer price for the next 40 TB of data transferred.

In this example, three separate AWS accounts transferred different amounts of data in Amazon S3 during the current month:

- Account 1 transferred 2 TB of data.
- Account 2 transferred 5 TB of data.
- Account 3 transferred 7 TB of data.

Because no single account passed the 10 TB threshold, none of them is eligible for the lower per-GB transfer price for the next 40 TB of data transferred.

Example: Volume pricing in Amazon S3



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

298

Now, suppose that the three accounts are linked in a single AWS organization and use consolidated billing.

When the Amazon S3 usage for the three linked accounts is combined ($2+5+7$), it results in a combined data transfer amount of 14 TB. This exceeds the 10-TB threshold.

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

In this example, Account 3 would receive a greater portion of the overall volume discount because at 7 TB, it transferred more data than Account 1 (at 2 TB) and Account 2 (at 5 TB).

AWS pricing tools

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



Next, you will examine pricing tools that you can use for budgeting and analyzing your AWS costs.

AWS Budgets

The AWS Budgets interface shows a list of budgets. The first four budgets (Project Nemo Cost Budget, Eastern US Regional Budget, Total Monthly Cost Budget, and Total EC2 Cost Budget) are highlighted with a pink border. The fifth budget, S3 Usage Budget, is not highlighted.

Budget name	Budget type	Current	Budgeted	Forecasted	Current vs. budgeted	Forecasted vs. budgeted
Project Nemo Cost Budget	Cost	\$43.90	\$45.00	\$56.33	97.55%	125.17%
Eastern US Regional Budget	Cost	\$85.21	\$100.00	\$125.28	85.21%	125.28%
Total Monthly Cost Budget	Cost	\$141.50	\$175.00	\$187.00	80.86%	106.86%
Total EC2 Cost Budget	Cost	\$136.90	\$200.00	\$195.21	68.45%	97.61%
S3 Usage Budget	Usage	3,601 Requests	5,500 Requests	4,675.75 Requests	65.47%	85.01%

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

In **AWS Budgets**, you can create budgets to plan your service usage, service costs, and instance reservations.

The information in AWS Budgets updates three times a day. This helps you to accurately determine how close your usage is to your budgeted amounts or to the AWS Free Tier limits.

In AWS Budgets, you can also set custom alerts when your usage exceeds (or is forecasted to exceed) the budgeted amount.

Suppose that you set a budget for Amazon EC2. You want to ensure that your company's usage of Amazon EC2 does not exceed \$200 for the month.

In AWS Budgets, you could set a custom budget to notify you when your usage reaches half of this amount (\$100). You would receive an alert and then decide how to proceed.

<click> This sample budget includes the following details:

- Current cost that you have incurred for Amazon EC2 so far this month (\$136.90)

- Forecasted cost for the month (\$195.21), based on usage patterns

<click> You can also compare your current and budgeted usage, and forecasted and budgeted usage. For example, in the top row of this sample budget, the forecasted vs. budgeted bar is at 125.17%. The reason for the increase is that the forecasted amount (\$56.33) exceeds the amount budgeted for that item for the month (\$45.00).

AWS Cost Explorer

The AWS Cost Explorer is a tool that you can use to visualize, understand, and manage your AWS costs and usage over time.

Instance Type	Oct 1, 2018	Nov 1, 2018	Dec 1, 2018	Jan 1, 2019	Feb 1, 2019	Mar 1, 2019
Total cost (\$)	1,312.71	1,328.54	1,125.99	1,129.85	1,092.63	1,092.27
t2.micro (\$)	486.75	479.89	405.63	409.27	396.11	396.11
c4.xlarge (\$)	296.11	286.56	296.11	296.11	296.11	296.11

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved. 301

AWS Cost Explorer is a tool that you can use to visualize, understand, and manage your AWS costs and usage over time.

AWS Cost Explorer includes a default report of the costs and usage for your top five cost-accruing AWS services. You can apply custom filters and groups to analyze your data. For example, you can view resource usage at the hourly level.

This example of the AWS Cost Explorer dashboard displays monthly costs for Amazon EC2 instances over a 6-month period. The bar for each month separates the costs for different Amazon EC2 instance types (such as t2.micro or m3.large).

By analyzing your AWS costs over time, you can make informed decisions about future costs and how to plan your budgets.

AWS Support plans

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



This section examines AWS Support plans. AWS offers four Support plans to help you troubleshoot issues, lower costs, and efficiently use AWS services. You can choose from the following Support plans to meet your company's needs: Basic, Developer, Business, and Enterprise.

Basic Support



Basic Support is free for all AWS customers and includes access to:

- Technical papers, documentation, and support communities
- AWS Personal Health Dashboard
- Seven core AWS Trusted Advisor checks



Basic Support is free for all AWS customers. It includes access to technical papers, documentation, and support communities. With Basic Support, you can also contact AWS for billing questions and service limit increases.

With Basic Support, you have a limited selection of AWS Trusted Advisor checks. Additionally, you can use the **AWS Personal Health Dashboard**, a tool that provides alerts and remediation guidance when AWS is experiencing events that might affect you.

If your company needs additional support, consider purchasing Developer, Business, or Enterprise Support.

AWS Support plans



Developer

- Best-practice guidance
- Client-side diagnostic tools
- Building-block architecture support

Business

- Use-case guidance
- All AWS Trusted Advisor checks
- Limited support for third-party software

Enterprise

- Application architecture guidance
- Infrastructure event management
- Technical Account Manager (TAM)

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

3/4

The Developer, Business, and Enterprise Support plans include all the benefits of Basic Support, in addition to the ability to open an unrestricted number of technical support cases. These three plans have pay-by-the-month pricing and require no long-term contracts.

The information in this course highlights only a selection of details for each plan. A complete overview of what is included in each plan, including pricing, is available on the AWS Support site.

In general, for pricing, the Developer plan has the lowest cost, the Business plan is in the middle, and the Enterprise plan has the highest cost.

Customers in the **Developer Support** plan have access to features such as:

- Best practice guidance
- Client-side diagnostic tools
- Building-block architecture support, which consists of guidance for how to use AWS offerings, features, and services together

For example, suppose that your company is exploring AWS services. You are unsure of how to use AWS services together to build applications that can address your company's needs. In this scenario, the building-block architecture support that is included with the Developer Support plan could help you identify opportunities for combining specific services and features.

Customers with a **Business Support** plan have access to additional features, including:

- Use-case guidance to identify AWS offerings, features, and services that can support your specific needs
- All AWS Trusted Advisor checks
- Limited support for third-party software, such as common operating systems and application stack components

Suppose that your company has the Business Support plan and wants to install a common third-party operating system onto your Amazon EC2 instances. You could contact AWS Support for assistance with installing, configuring, and troubleshooting the operating system. For advanced topics such as optimizing performance, using custom scripts, or resolving security issues, you might need to contact the third-party software provider directly.

In addition to all the features included in the Basic, Developer, and Business Support plans, customers with an **Enterprise Support** plan have access to features such as:

- Application architecture guidance, which is a consultative relationship to support your company's specific use cases and applications
- Infrastructure event management (A short-term engagement with AWS Support that helps your company gain a better understanding of your use cases. This also provides your company with architectural and scaling guidance.)
- Technical Account Manager

Technical Account Manager (TAM)



The **Technical Account Manager** is your primary point of contact at AWS.

- Technical Account Managers are included only with the Enterprise Support plan.
- They provide guidance, technical expertise, and best practices.



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

305

The Enterprise Support plan includes access to a **Technical Account Manager (TAM)**.

If your company has an Enterprise Support plan, the TAM is your primary point of contact at AWS. They provide guidance, architectural reviews, and ongoing communication with your company as you plan, deploy, and optimize your applications.

Your TAM provides expertise across the full range of AWS services. They help you design solutions that efficiently use multiple services together through an integrated approach.

For example, suppose that you are interested in developing an application that uses several AWS services together. Your TAM could provide insights into how to use the services together. They achieve this, while aligning with the specific needs that your company is hoping to address through the new application.

Knowledge check question



306.

Which of the following is the lowest-cost AWS Support plan that includes all AWS Trusted Advisor checks?

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

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which of the following is the lowest-cost AWS Support plan that includes all AWS Trusted Advisor checks?

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

Knowledge check answer



307

Which of the following is the lowest-cost AWS Support plan that includes all AWS Trusted Advisor checks?

- A. Business (correct)
- B. Developer
- C. Enterprise
- D. Basic

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct answer is **A. Business**.

Only the Business and Enterprise Support plans include all AWS Trusted Advisor checks. Of these two Support plans, the Business Support plan has a lower cost.

AWS Marketplace

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



As you continue to explore AWS services, you might consider using them together with third-party software. This might include software that you are already using and want to integrate into AWS services, or new software that can help you create innovative solutions for your customers.

To find third-party software that you can use with AWS services, visit the **AWS Marketplace**.

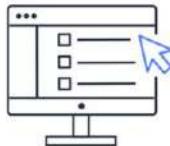
AWS Marketplace



AWS Marketplace is a digital catalog that provides listings of third-party software that runs on AWS.



Discover thousands of software products that run on AWS



Access detailed information and reviews for each product listing



Explore software solutions by industry and use case

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

309

AWS Marketplace is a digital catalog that includes thousands of software listings from independent software vendors. You can use AWS Marketplace to find, test, and buy software that runs on AWS.

For each listing in AWS Marketplace, you can access detailed information on pricing options, available support, and reviews from other AWS customers.

You can also explore software solutions by industry and use case. For example, suppose that your company is in the healthcare industry. In the AWS Marketplace, you can review use cases that software helps you address, such as implement solutions to protect patient records, or use machine learning models to analyze a patient's medical history and predict possible health risks.

AWS Marketplace categories



Business Applications



Data and Analytics



DevOps



Infrastructure Software



Internet of Things (IoT)



Machine Learning



Migration



Security

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

310

AWS Marketplace offers products in several categories, such as Infrastructure Products, Business Applications, Data Products, and DevOps.

In each category, you can browse through product listings in subcategories. For example, subcategories in the DevOps category include areas such as Application Development, Monitoring, and Testing.

Module 8

Knowledge check

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



Knowledge check question 1



312

Which action can a customer perform with consolidated billing?

- A. Review how much cost predicted AWS usage will incur by the end of the month
- B. Create an estimate for the cost of use cases on AWS
- C. Combine usage across accounts to receive volume pricing discounts
- D. Visualize and manage AWS costs and usage over time

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which action can a customer perform with consolidated billing?

- A. Review how much cost predicted AWS usage will incur by the end of the month
- B. Create an estimate for the cost of use cases on AWS
- C. Combine usage across accounts to receive volume pricing discounts
- D. Visualize and manage AWS costs and usage over time

Knowledge check answer 1



315

Which action can a customer perform with consolidated billing?

- A. Review how much cost predicted AWS usage will incur by the end of the month
- B. Create an estimate for the cost of use cases on AWS
- C. **Combine usage across accounts to receive volume pricing discounts (correct)**
- D. Visualize and manage AWS costs and usage over time

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **C. Combine usage across accounts to receive volume pricing discounts.**

The other response options are incorrect because:

- A. You can perform this action in *AWS Budgets*.
- B. You can perform this action in *AWS Pricing Calculator*.
- D. You can perform this action in *AWS Cost Explorer*.

Knowledge check question 2



314

Which pricing tool is used to visualize, understand, and manage AWS costs and usage over time?

- A. AWS Pricing Calculator
- B. AWS Budgets
- C. AWS Cost Explorer
- D. AWS Free Tier

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which pricing tool is used to visualize, understand, and manage AWS costs and usage over time?

- A. AWS Pricing Calculator
- B. AWS Budgets
- C. AWS Cost Explorer
- D. AWS Free Tier

Knowledge check answer 2



315

Which pricing tool is used to visualize, understand, and manage your AWS costs and usage over time?

- A. AWS Pricing Calculator
- B. AWS Budgets
- C. **AWS Cost Explorer (correct)**
- D. AWS Free Tier

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **C. AWS Cost Explorer**.

AWS Cost Explorer includes a default report of the costs and usage for your top five cost-accruing AWS services. You can apply custom filters and groups to analyze your data. For example, you can view resource usage at the hourly level.

The other response options are incorrect because:

- A. You can use AS Pricing Calculator to create an estimate for the cost of your use cases on AWS.
- B. AWS Budgets lets you create budgets to plan your service usage, service costs, and instance reservations. In AWS Budgets, you can also set custom alerts when your usage exceeds (or is forecasted to exceed) the budgeted amount.
- D. The AWS Free Tier is a program that consists of three types of offers that allow customers to use AWS services without incurring costs: Always Free, 12 Months Free, and Trials.

Knowledge check question 3



316.

Which pricing tool can a customer use to receive alerts when their service usage exceeds a customer-defined threshold?

- A. Billing dashboard in the AWS Management Console
- B. AWS Budgets
- C. AWS Free Tier
- D. AWS Cost Explorer

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which pricing tool can a customer use to receive alerts when their service usage exceeds a customer-defined threshold?

- A. Billing dashboard in the AWS Management Console
- B. AWS Budgets
- C. AWS Free Tier
- D. AWS Cost Explorer

Knowledge check answer 3



317

Which pricing tool can a customer use to receive alerts when their service usage exceeds a customer-defined threshold?

- A. Billing dashboard in the AWS Management Console
- B. AWS Budgets (correct)**
- C. AWS Free Tier
- D. AWS Cost Explorer

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **B. AWS Budgets**.

In AWS Budgets, you can set custom alerts that will notify you when your service usage exceeds (or is forecasted to exceed) the amount that you have budgeted.

Your budget can be based on costs or usage. For example, you can set an alert that will notify you when you have incurred \$100.00 of costs in Amazon EC2 or 500,000 requests in AWS Lambda.

The other response options are incorrect because:

- A. From the billing dashboard in the AWS Management Console, you can view details on your AWS bill, such as service costs by Region, month to date spend, and more. However, you cannot set alerts from the billing dashboard.
- C. The AWS Free Tier is a program that consists of three types of offers that allow customers to use AWS services without incurring costs: Always Free, 12 Months Free, and Trials.

D. AWS Cost Explorer is a tool that you can use to visualize, understand, and manage your AWS costs and usage over time.

Knowledge check question 4



318.

A company wants to receive support from an AWS Technical Account Manager (TAM). Which support plan should they choose?

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

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Knowledge check answer 4



319

A company wants to receive support from an AWS Technical Account Manager (TAM). Which support plan should they choose?

- A. Developer
- B. Basic
- C. Enterprise (correct)**
- D. Business

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **C. Enterprise**.

A Technical Account Manager (TAM) is available only to AWS customers with an Enterprise Support plan. A TAM provides guidance, architectural reviews, and ongoing communication with your company as you plan, deploy, and optimize your applications.

Knowledge check question 5



320

Which service or resource is used to find third-party software that runs on AWS?

- A. AWS Marketplace
- B. AWS Free Tier
- C. AWS Support
- D. Billing dashboard in the AWS Management Console

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which service or resource is used to find third-party software that runs on AWS?

- A. AWS Marketplace
- B. AWS Free Tier
- C. AWS Support
- D. Billing dashboard in the AWS Management Console

Knowledge check answer 5



321

Which service or resource is used to find third-party software that runs on AWS?

- A. **AWS Marketplace (correct)**
- B. AWS Free Tier
- C. AWS Support
- D. Billing dashboard in the AWS Management Console

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **A. AWS Marketplace**.

AWS Marketplace is a digital catalog that includes thousands of software listings from independent software vendors. You can use AWS Marketplace to find, test, and buy software that runs on AWS.

The other response options are incorrect because:

- B. The AWS Free Tier consists of offers that allow customers to use AWS services without incurring costs. These offers are related to AWS services, not third-party software that can be used on AWS.
- C. AWS Support is a resource that can answer questions about best practices, assist with troubleshooting issues, help you to identify ways to optimize your use of AWS services, and so on.
- D. You can use the billing dashboard in the AWS Management Console to view details such as service costs by Region, the top services being used by your account, and forecasted billing costs. From the billing dashboard, you can also access other AWS

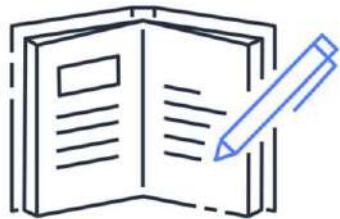
billing tools, such as AWS Cost Explorer, AWS Budgets, and AWS Budgets Reports.

Module 8 summary



In this module, you learned about:

- AWS Free Tier
- Consolidated billing
- Tools for planning, estimating, and reviewing AWS costs
- AWS Support plans
- AWS Marketplace benefits



In this module, you learned about the following concepts:

- Three types of offers included in the AWS Free Tier: Always Free, 12 Months Free, and Trials
- Benefits of consolidated billing in AWS Organizations
- Tools for planning, estimating, and reviewing AWS costs
- Differences between the four AWS Support plans: Basic, Developer, Business, and Enterprise
- Benefits of AWS Marketplace

The next module examines migration and innovation in the AWS Cloud.

Module 9

Migration and Innovation



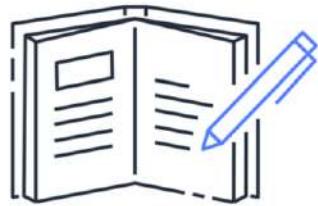
In this module, you will learn about migration and innovation on AWS. This includes migration services, cloud migration strategies, and the AWS Cloud Adoption Framework.

Module 9 objectives



In this module, you will learn how to:

- Describe migration and innovation in the AWS Cloud
- Summarize the AWS Cloud Adoption Framework (AWS CAF)
- Summarize the six key factors of a cloud migration strategy
- Describe the benefits of AWS data migration solutions
- Summarize the broad scope of innovative solutions that AWS offers
- Summarize the five pillars of the AWS Well-Architected Framework



In this module, you will learn how to:

- Describe migration and innovation in the AWS Cloud
- Summarize the AWS Cloud Adoption Framework (AWS CAF)
- Summarize the six key factors of a cloud migration strategy
- Describe the benefits of AWS data migration solutions
- Summarize the broad scope of innovative solutions that AWS offers
- Summarize the five pillars of the AWS Well-Architected Framework

AWS Cloud Adoption Framework

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



In this section, you will explore the AWS Cloud Adoption Framework, which provides guidance to support organizational change throughout the cloud adoption process.

- Provides advice to your company to enable a quick and smooth migration to AWS
- Organizes guidance into six areas of focus, called **perspectives**



Migrating to the cloud is a process. You don't snap your fingers and have everything magically hosted in AWS. Migrating applications takes effort, and a successful cloud migration requires expertise.

Fortunately, many people have successfully migrated to AWS, and a lot of knowledge about the process has been captured and shared.

That being said, the position you hold in your organization will impact what you need to know and how you can help with a migration. If you are a developer, your role and viewpoint will be much different than a cloud architect, business analyst, or financial analyst. Different types of people bring different perspectives to the table for a migration. You want to harness those different perspectives and make sure that everyone has the same focus.

You also want to ensure that you have the right talent to help support your migration. HR will need to hire at the correct rate to enable your migration. This can be a lot to track, and someone new to the cloud might not think of all the different people who need to be involved.

The AWS Professional Services team created the **AWS Cloud Adoption Framework (AWS CAF)** to help you manage this process. The Cloud Adoption Framework provides advice to your company to enable a smooth migration to AWS.

At the highest level, the AWS CAF organizes guidance into six areas of focus, called **perspectives**. Each perspective addresses distinct responsibilities. The planning process helps the right people across the organization prepare for the changes ahead.

Perspectives



Each perspective of the AWS CAF addresses distinct responsibilities. The planning process helps the right people across the organization prepare for the changes ahead. In general, the **Business**, **People**, and **Governance** perspectives focus on business capabilities, whereas the **Platform**, **Security**, and **Operations** perspectives focus on technical capabilities. For example, someone who is a business or finance analysts is part of the Business perspective, HR is part of the People perspective, and a cloud architect is part of the Platform perspective.

Each perspective uncovers gaps in your skills and processes, which are then recorded as inputs. The inputs are then used as the basis for creating an **AWS Cloud Adoption Framework Action Plan**. You can use the action plan to guide your organization's change management as you journey to the cloud. Having an action plan that makes sense for your organization can help keep you on track towards achieving your desired outcomes.

Business perspective



Business



People



Governance



Platform



Security



Operations



Goal

Ensures that IT aligns with business needs and IT investments link to key business results

Common roles

- Business managers
- Finance managers
- Budget owners
- Strategy stakeholders

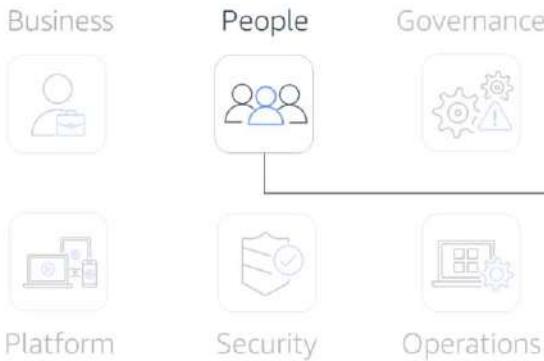
The **Business perspective** ensures that IT aligns with business needs and IT investments link to key business results.

Use the Business perspective to create a strong business case for cloud adoption and prioritize cloud adoption initiatives. Ensure that your business strategies and goals align with your IT strategies and goals.

Common roles in the Business perspective include:

- Business managers
- Finance managers
- Budget owners
- Strategy stakeholders

People perspective



Goal

Supports development of an organization-wide change management strategy for successful cloud adoption

Common roles

- Human resources
- Staffing
- People managers

The **People perspective** supports development of an organization-wide change management strategy for successful cloud adoption.

Use the People perspective to evaluate organizational structures and roles, new skill and process requirements, and identify gaps. This helps prioritize training, staffing, and organizational changes.

Common roles in the People perspective include:

- Human resources
- Staffing
- People managers

Governance perspective



Goal

Focuses on the skills and processes to align IT strategy with business strategy

Common roles

- Chief information officer (CIO)
- Program managers
- Enterprise architects
- Business analysts
- Portfolio managers

The **Governance perspective** focuses on the skills and processes to align IT strategy with business strategy. This ensures that you maximize the business value and minimize risks.

Use the Governance perspective to understand how to update the staff skills and processes necessary to ensure business governance in the cloud. Manage and measure cloud investments to evaluate business outcomes.

Common roles in the Governance perspective include:

- Chief information officer (CIO)
- Program managers
- Enterprise architects
- Business analysts
- Portfolio managers

Platform perspective



Business



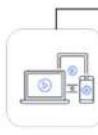
People



Governance



Platform



Security



Operations



Goal

Includes principles and patterns for implementing new solutions in the cloud, and migrating on-premises workloads to the cloud

Common roles

- Chief technology officer (CTO)
- IT managers
- Solutions architects

The **Platform perspective** includes principles and patterns for implementing new solutions in the cloud, and migrating on-premises workloads to the cloud.

Use a variety of architectural models to understand and communicate the structure of IT systems and their relationships. Describe the architecture of the target state environment in detail.

Common roles in the Platform perspective include:

- Chief technology officer (CTO)
- IT managers
- Solutions architects

Security perspective



Goal

Ensures that the organization meets security objectives for visibility, auditability, control, and agility

Common roles

- Chief information security officer (CISO)
- IT security managers
- IT security analysts

The **Security perspective** ensures that an organization meets security objectives for visibility, auditability, control, and agility.

Use the AWS CAF to structure the selection and implementation of security controls that meet the organization's needs.

Common roles in the Security perspective include:

- Chief information security officer (CISO)
- IT security managers
- IT security analysts

Operations perspective



Goal

Helps you to enable, run, use, operate, and recover IT workloads to the level agreed on with your business stakeholders

Common roles

- IT operations managers
- IT support managers

The **Operations perspective** helps you to enable, run, use, operate, and recover IT workloads to the level agreed on with your business stakeholders.

Define how day-to-day, quarter-to-quarter, and year-to-year business is conducted. Align with and support the operations of the business. The AWS CAF helps stakeholders define current operating procedures and identify the process changes and training needed to implement successful cloud adoption.

Common roles in the Operations perspective include:

- IT operations managers
- IT support managers

Migrating to the cloud can be complicated, but you are not alone in this. You have access to many resources that can help you get started, and the AWS Cloud Adoption Framework is a helpful place to look.

Knowledge check question



334

Which AWS Cloud Adoption Framework perspective helps customers design, implement, and optimize their AWS solution based on their business goals and perspectives?

- A. Business perspective
- B. Platform perspective
- C. Operations perspective
- D. People perspective

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which AWS Cloud Adoption Framework perspective helps customers design, implement, and optimize their AWS solution based on their business goals and perspectives?

- A. Business perspective
- B. Platform perspective
- C. Operations perspective
- D. People perspective

Knowledge check answer



335

Which AWS Cloud Adoption Framework perspective helps customers design, implement, and optimize their AWS solution based on their business goals and perspectives?

- A. Business perspective
- B. Platform perspective (correct)
- C. Operations perspective
- D. People perspective

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **B. Platform perspective**.

The Platform perspective of the AWS Cloud Adoption Framework also includes principles for implementing new solutions and migrating on-premises workloads to the cloud.

The other response options are incorrect because:

- A. The Business perspective helps you move from a model that separates business and IT strategies into a business model that integrates IT strategy.
- C. The Operations perspective focuses on operating and recovering IT workloads to meet the requirements of business stakeholders.
- D. The People perspective helps Human Resources employees prepare their teams for cloud adoption by updating organizational processes and staff skills to include cloud-based competencies.

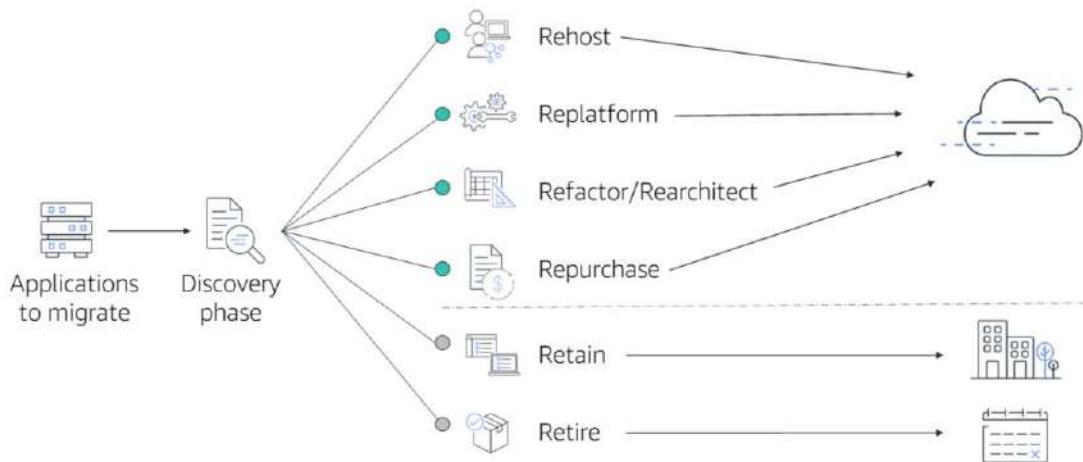
Migration strategies

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



This section examines six strategies that you can consider implementing when preparing for a cloud migration.

Six migration strategies



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

337

Suppose that you want to migrate from your on-premises deployment to AWS. Ideally, you could snap your fingers and instantly have all the elements from your existing on-premises data center magically appear on AWS, optimized and efficient. However, migrating doesn't work that way.

Every application (or application groups, if they're tightly coupled) has six possible options for a migration. These are known as the **six Rs of migration**. Once you complete the discovery phase and know exactly what is present in your existing environment, decide which of the six Rs might be the best option, based on factors such as time, cost, priority, and criticality.

When migrating applications to the cloud, six of the most common migration strategies that you can implement are:

- Rehosting
- Replatforming
- Refactoring/re-architecting
- Repurchasing
- Retaining

- Retiring

Rehosting (also known as *lift and shift*) involves moving applications without changes. In the scenario of a large legacy migration, in which the company is looking to implement its migration and scale quickly to meet a business case, the majority of applications are rehosted.

<click> Replatforming (also known as *lift, tinker, and shift*) involves making a few cloud optimizations to realize a tangible benefit. Optimization is achieved without changing the core architecture of the application.

<click> Refactoring (also known as *rearchitecting*) involves reimagining how an application is architected and developed by using cloud-native features. Refactoring is driven by a strong business need to add features, scale, or performance that would otherwise be difficult to achieve in the application's existing environment.

<click> Repurchasing involves moving from a traditional license to a software as a service model. For example, a business might choose to implement the repurchasing strategy by migrating from a customer relationship management (CRM) system to Salesforce.com.

The final two strategies, retaining and retiring, do *not* involve moving applications to the cloud.

<click> Retaining consists of keeping applications that are critical for the business in the source environment. This might include applications that require major refactoring before they can be migrated, or, work that can be postponed until a later time.

<click> Retiring is the process of removing applications that are no longer needed.

Knowledge check question



338.

Which migration strategy involves moving from a traditional license to a software as a service model?

- A. Refactoring
- B. Retiring
- C. Replatforming
- D. Repurchasing

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which migration strategy involves moving from a traditional license to a software as a service model?

- A. Refactoring
- B. Retiring
- C. Replatforming
- D. Repurchasing

Knowledge check answer



339

Which migration strategy involves moving from a traditional license to a software as a service model?

- A. Refactoring
- B. Retiring
- C. Replatforming
- D. **Repurchasing (correct)**

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **D: Repurchasing**.

Repurchasing involves replacing an existing application with a cloud-based version, such as software found in AWS Marketplace.

The other response options are incorrect because:

- A. Refactoring involves changing how an application is architected and developed, typically by using cloud-native features.
- B. Retiring involves removing an application that is no longer used or that can be turned off.
- C. Replatforming involves selectively optimizing aspects of an application to achieve benefits in the cloud without changing the core architecture of the application. It is also known as lift, tinker, and shift.

AWS Snow Family

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



Suppose that you have a large amount of data that you need to transfer into the AWS Cloud. For this type of workload, you can use devices that are part of the **AWS Snow Family**. The AWS Snow Family is a collection of physical devices that help to physically transport up to exabytes of data into and out of AWS.

AWS Snow Family



AWS Snowcone

- Small, rugged, and secure edge computing and data transfer device
- Features 8 TB of usable storage

AWS Snowball devices

- AWS Snowball Edge Storage Optimized
- AWS Snowball Edge Compute Optimized

AWS Snowmobile

- Exabyte-scale data transfer service for moving large amounts of data to AWS
- Transfers up to 100 PB of data

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

341

The AWS Snow Family is composed of **AWS Snowcone**, **AWS Snowball**, and **AWS Snowmobile**. These devices offer different capacity points, and most include built-in computing capabilities. AWS owns and manages the Snow Family devices and integrates with AWS security, monitoring, storage management, and computing capabilities.

AWS Snowcone is a small, rugged, and secure edge computing and data transfer device. It features 2 CPUs, 4 GB of memory, and 8 TB of usable storage.

<click> AWS offers two types of **AWS Snowball** devices:

- **Snowball Edge Storage Optimized** devices are well suited for large-scale data migrations and recurring transfer workflows, in addition to local computing with higher capacity needs.
 - Storage: 80 TB of hard disk drive (HDD) capacity for block volumes and Amazon S3 compatible object storage; 1 TB of SATA solid state drive (SSD) for block volumes
 - Compute: 40 vCPUs; 80 GiB of memory to support Amazon EC2 sbe1

instances (equivalent to C5)

- **Snowball Edge Compute Optimized** provides powerful computing resources for use cases such as machine learning, full motion video analysis, analytics, and local computing stacks.
 - Storage: 42-TB usable HDD capacity for Amazon S3 compatible object storage or Amazon EBS compatible block volumes; 7.68 TB of usable NVMe SSD capacity for Amazon EBS compatible block volumes
 - Compute: 52 vCPUs; 208 GiB of memory; optional NVIDIA Tesla V100 GPU; run Amazon EC2 sbe-c and sbe-g instances, which are equivalent to C5, M5a, G3, and P3 instances

<click> AWS Snowmobile is an exabyte-scale data transfer service used to move large amounts of data to AWS. You can transfer up to 100 petabytes of data per Snowmobile, which is a 45-foot long ruggedized shipping container, pulled by a semitrailer truck.

Innovation with AWS

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



The final section of this module examines innovation with AWS.

Driving innovation in the cloud involves clearly articulating the following conditions:

- Current state
- Desired state
- Problems you are trying to solve



When examining how to use AWS services, focus on the desired outcomes. You are properly equipped to drive innovation in the cloud if you can clearly articulate the following:

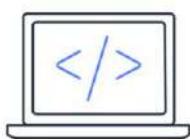
- Current state
- Desired state
- Problems you are trying to solve

Consider some of the paths you might explore in the future as you continue on your cloud journey.

Innovation paths



Consider some of the following innovation paths as you continue on your cloud journey.



Serverless applications



Artificial intelligence (AI)



Machine learning (ML)

Serverless applications: With AWS, **serverless** refers to applications that don't require you to provision, maintain, or administer servers. AWS handles fault tolerance and availability for you.

AWS Lambda is an example of a service that you can use to run serverless applications. If you design your architecture to trigger Lambda functions to run your code, you can bypass the need to manage a fleet of servers. Building your architecture with serverless applications helps developers focus on their core product instead of managing and operating servers.

Artificial intelligence (AI): AWS offers a variety of services powered by AI. For example, you can:

- Convert speech to text with Amazon Transcribe
- Discover patterns in text with Amazon Comprehend
- Identify potentially fraudulent online activities with Amazon Fraud Detector
- Build voice and text chatbots with Amazon Lex

Machine learning (ML): Traditional machine learning development is complex,

expensive, time consuming, and error prone. AWS offers Amazon SageMaker to remove the difficult work from the process and empower you to build, train, and deploy ML models quickly. You can use ML to analyze data, solve complex problems, and predict outcomes.

AWS Well-Architected Framework

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



Throughout this course, you have learned about a wide range of AWS services. You can use these services as building blocks for your cloud architecture. To help you evaluate how well your architecture aligns with best practices, you can use the **Well-Architected Framework**.

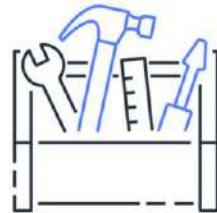
Well-Architected Framework



The **Well-Architected Framework** helps you understand how to design and operate reliable, secure, efficient, and cost-effective systems in the AWS Cloud.

It is based on five pillars:

- Operational excellence
- Security
- Reliability
- Performance efficiency
- Cost optimization



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

340

The Well-Architected Framework helps you understand how to design and operate reliable, secure, efficient, and cost-effective systems in the AWS Cloud. It provides a way for you to consistently measure your architecture against best practices and design principles and identify areas for improvement.

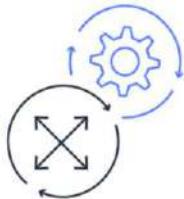
The Well-Architected Framework is based on five pillars:

- Operational excellence
- Security
- Reliability
- Performance efficiency
- Cost optimization

Operational excellence



Run and monitor systems to deliver business value and to continually improve supporting processes and procedures



- Perform operations as code
- Annotate documentation
- Anticipate failure
- Refine operations procedures frequently
- Make frequent, small, reversible changes

The first pillar is **operational excellence**. It focuses on running and monitoring systems to deliver business value, and with that, continually improving processes and procedures. For example, automating changes with deployment pipelines, or responding to events that are triggered.

Design principles for operational excellence in the cloud include performing operations as code, annotating documentation, anticipating failure, and frequently making small, reversible changes.

Security



Protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies



- Automate security best practices
- Apply security at all layers
- Protect data in transit and at rest

The **security** pillar is the ability to protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies.

When considering the security of your architecture, apply these best practices:

- Automate security best practices when possible
- Apply security at all layers
- Protect data in transit and at rest

Reliability



Test recovery procedures, scale horizontally to increase aggregate system availability, and automatically recover from failure



- Recover from infrastructure or service disruptions
- Dynamically acquire computing resources to meet demand
- Mitigate disruptions such as misconfigurations or transient network issues

Reliability is the ability of a system to do the following:

- Recover from infrastructure or service disruptions
- Dynamically acquire computing resources to meet demand
- Mitigate disruptions such as misconfigurations or transient network issues

Reliability includes testing recovery procedures, scaling horizontally to increase aggregate system availability, and automatically recovering from failure.

Performance efficiency



Use computing resources efficiently to meet system requirements and maintain that efficiency as demand changes and technologies evolve



- Experiment more often
- Use serverless architectures
- Go global in minutes

Performance efficiency is the ability to use computing resources efficiently to meet system requirements, and maintain that efficiency as demand changes and technologies evolve. An example of performance efficiency is choosing the right Amazon EC2 instance type for an application.

Evaluating the performance efficiency of your architecture includes experimenting more often, using serverless architectures, and designing systems to be able to go global in minutes.

Cost optimization



Run systems to deliver business value at the lowest price point



- Adopt a consumption model
- Analyze and attribute expenditure
- Use managed services to reduce cost of ownership

Cost optimization is the ability to run systems to deliver business value at the lowest price point. For example, suppose that you are analyzing your Amazon EC2 compute usage. If you have overestimated your compute needs, you could lower your costs by choosing a more cost-effective instance type.

Cost optimization includes adopting a consumption model, analyzing and attributing expenditure, and using managed services to reduce the cost of ownership.

Module 9

Knowledge check

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



Knowledge check question 1



355

Which AWS Cloud Adoption Framework perspective helps you structure the selection and implementation of permissions?

- A. Governance perspective
- B. Security perspective
- C. Operations perspective
- D. Business perspective

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which AWS Cloud Adoption Framework perspective helps you structure the selection and implementation of permissions?

- A. Governance perspective
- B. Security perspective
- C. Operations perspective
- D. Business perspective

Knowledge check answer 1



354

Which AWS Cloud Adoption Framework perspective helps you structure the selection and implementation of permissions?

- A. Governance perspective
- B. Security perspective (correct)**
- C. Operations perspective
- D. Business perspective

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **B. Security perspective**.

The Security perspective of the AWS Cloud Adoption Framework also helps you identify areas of non-compliance and plan ongoing security initiatives.

The other response options are incorrect because:

- A. Governance perspective helps you identify and implement best practices for IT governance and support business processes with technology.
- C. Operations perspective focuses on operating and recovering IT workloads to meet the requirements of business stakeholders.
- D. Business perspective helps you move from a model that separates business and IT strategies into a business model that integrates IT strategy.

Knowledge check question 2



355

Which strategies are included in the six strategies for application migration? (Select TWO.)

- A. Revisiting
- B. Retaining
- C. Remembering
- D. Redeveloping
- E. Rehosting

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which strategies are included in the six strategies for application migration? (Select TWO.)

- A. Revisiting
- B. Retaining
- C. Remembering
- D. Redeveloping
- E. Rehosting

Knowledge check answer 2



356.

Which strategies are included in the six strategies for application migration? (Select TWO.)

- A. Revisiting
- B. **Retaining (correct)**
- C. Remembering
- D. Redeveloping
- E. **Rehosting (correct)**

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The two correct response options are:

- **B. Retaining**
- **E. Rehosting**

The application migration strategies are rehosting, replatforming, refactoring/rearchitecting, repurchasing, retaining, and retiring.

Knowledge check question 3



357

What is the storage capacity of AWS Snowmobile?

- A. 40 PB
- B. 60 PB
- C. 80 PB
- D. 100 PB

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is the storage capacity of AWS Snowmobile?

- A. 40 PB
- B. 60 PB
- C. 80 PB
- D. 100 PB

Knowledge check answer 3



358

What is the storage capacity of AWS Snowmobile?

- A. 40 PB
- B. 60 PB
- C. 80 PB
- D. **100 PB (correct)**

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **D. 100 PB**.

AWS Snowmobile is a service that is used for transferring up to 100 PB of data to AWS. Each Snowmobile is a 45-foot long shipping container that is pulled by a semitrailer truck.

Knowledge check question 4



359

What is the storage capacity of Snowball Edge Storage Optimized?

- A. 40 TB
- B. 60 TB
- C. 80 TB
- D. 100 TB

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is the storage capacity of Snowball Edge Storage Optimized?

- A. 40 TB
- B. 60 TB
- C. 80 TB
- D. 100 TB

Knowledge check answer 4



360

What is the storage capacity of Snowball Edge Storage Optimized?

- A. 40 TB
- B. 60 TB
- C. **80 TB (correct)**
- D. 100 TB

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **C. 80 TB**.

Snowball Edge Storage Optimized is a device that you can use to transfer large amounts of data into and out of AWS. It provides 80 TB of usable HDD storage.

Knowledge check question 5



361

Which AWS Well-Architected Framework pillar includes the ability to recover from infrastructure or service disruptions?

- A. Cost optimization
- B. Operational excellence
- C. Performance efficiency
- D. Reliability

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which AWS Well-Architected Framework pillar includes the ability to recover from infrastructure or service disruptions?

- A. Cost optimization
- B. Operational excellence
- C. Performance efficiency
- D. Reliability

Knowledge check answer 5



362

Which AWS Well-Architected Framework pillar includes the ability to recover from infrastructure or service disruptions?

- A. Cost optimization
- B. Operational excellence (correct)**
- C. Performance efficiency
- D. Reliability

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The correct response option is **B. Operational excellence**.

The other response options are incorrect because:

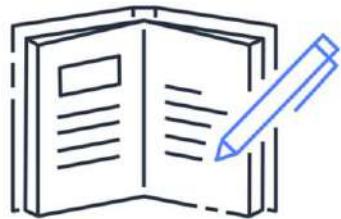
- A. The cost optimization pillar focuses on the ability to run systems to deliver business value at the lowest price point.
- C. The performance efficiency pillar focuses on using computing resources efficiently to meet system requirements, and maintain that efficiency as demand changes and technologies evolve.
- D. The reliability pillar focuses on the ability of a workload to consistently and correctly perform its intended functions.

Module 9 summary



In this module, you learned about:

- AWS Cloud Adoption Framework
- Six strategies for migration
- AWS Snow Family
- Innovation with AWS services
- Five pillars of the AWS Well-Architected Framework



In this module, you learned about the following concepts:

- AWS Cloud Adoption Framework (AWS CAF), which consists of six perspectives:
 - Business perspective
 - People perspective
 - Governance perspective
 - Platform perspective
 - Security perspective
 - Operations perspective
- Six strategies for migration:
 - Rehosting
 - Replatforming
 - Refactoring/Rearchitecting
 - Repurchasing
 - Retaining
 - Retiring
- AWS Snow Family, which consists of AWS Snowcone, AWS Snowball, and AWS

Snowmobile

- Innovation with AWS services through areas such as serverless applications, artificial intelligence (AI), and machine learning (ML)
- Five pillars of the AWS Well-Architected Framework:
 - Operational excellence
 - Security
 - Reliability
 - Performance efficiency
 - Cost optimization

The next module examines migration and innovation in the AWS Cloud.

Module 10

AWS Certified Cloud Practitioner Basics



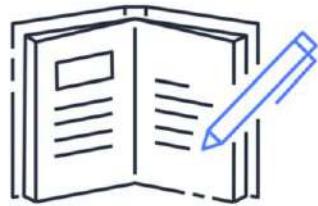
In this module, you will learn specific details and strategies to help you prepare for the AWS Certified Cloud Practitioner exam.

Module 10 objectives



In this module, you will learn how to:

- Determine resources for preparing for the AWS Certified Cloud Practitioner exam
- Evaluate types of questions that are included on the AWS Certified Cloud Practitioner exam



In this module, you will learn how to:

- Determine resources for preparing for the AWS Certified Cloud Practitioner exam
- Evaluate types of questions that are included on the AWS Certified Cloud Practitioner exam

Exam details

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



In this section, you will learn about the AWS Certified Cloud Practitioner exam, including exam domains, recommended experience, and additional resources.

Exam domains



Domain	% of Exam
Domain 1: Cloud Concepts	26%
Domain 2: Security and Compliance	25%
Domain 3: Technology	33%
Domain 4: Billing and Pricing	16%
Total	100%

Learn more at: <https://aws.amazon.com/certification/certified-cloud-practitioner>

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

367

The AWS Certified Cloud Practitioner exam includes four domains:

- Domain 1: Cloud Concepts
- Domain 2: Security and Compliance
- Domain 3: Technology
- Domain 4: Billing and Pricing

The areas covered describe each domain in the Exam Guide for the AWS Certified Cloud Practitioner certification. For a description of each domain, review the AWS Certified Cloud Practitioner website (<https://aws.amazon.com/certification/certified-cloud-practitioner>). You are encouraged to read the information in the Exam Guide as part of your preparation for the exam.

Each domain in the exam is weighted. The weight represents the percentage of questions in the exam that correspond to that particular domain. These are approximations, so the questions on your exam might not match these percentages exactly. The exam does not indicate the domain associated with a question. In fact, some questions can potentially fall under multiple domains.

You are encouraged to use these benchmarks to help you determine how to allocate your time studying for the exam.

Recommended experience



For this exam, you should have:

- Basic understanding of IT services
- At least 6 months experience with the AWS Cloud



Candidates for the AWS Certified Cloud Practitioner exam should have a basic understanding of IT services and their uses in the AWS Cloud platform.

We recommend that you have at least 6 months of experience with the AWS Cloud in any role, including project managers, IT managers, sales managers, decision makers, and marketers. These roles are in addition to those working in finance, procurement, and legal departments.

Exam details



- You must complete the exam within 90 minutes.
- The minimum passing score is 700 (the maximum score is 1,000).
- The exam consists of multiple choice and multiple response questions.
- The exam is available in English, Indonesian (Bahasa), Japanese, Korean, and Simplified Chinese.
- A 30-minute time extension is available upon request to non-native English speakers who are taking an exam in English.



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

368

The AWS Certified Cloud Practitioner exam must be completed within **90 minutes**. The minimum passing score is **700** (out of a maximum score of 1,000).

Two types of questions are included on the exam: multiple choice and multiple response.

- A **multiple-choice** question has one correct response and three incorrect responses, or *distractors*.
- A **multiple-response** question has two or more correct responses out of five or more options.

Currently, the exam is available in English, Indonesian (Bahasa), Japanese, Korean, and Simplified Chinese.

Additionally, a 30-minute time extension is available upon request to non-native English speakers who are taking an exam in English. The accommodation, “ESL +30,” only needs to be requested once, prior to registering for an exam. It will apply to all future exam registrations with all test delivery providers. For more information about how to request this accommodation, refer to

[https://aws.amazon.com/certification/policies/before-testing/#Scheduling_Exams.](https://aws.amazon.com/certification/policies/before-testing/#Scheduling_Exams)

Exam details



- There is no penalty for guessing.
- Unanswered questions are scored as incorrect.
- You can flag questions to review before submitting the exam.



On the exam, there is no penalty for guessing. Any questions that you do not answer will be scored as incorrect, so even if you are unsure of what the correct answer is, you should guess, rather than leave any questions unanswered.

The exam also lets you flag questions that you want to review before submitting the exam. This can help you to use your time during the exam more efficiently. You can always go back and review any questions that you were initially unsure of.

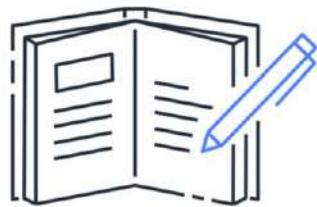
For more details on exam logistics and policies, refer to the AWS Certification FAQ (<https://aws.amazon.com/certification/faqs>). Additional details regarding identification requirements and system requirements for online proctoring will be included in the confirmation email that you receive from PSI or Pearson VUE after you register for the exam.

Technical papers and resources



We recommend that you review the following technical papers and resources:

- Overview of Amazon Web Services:
<https://d1.awsstatic.com/whitepapers/aws-overview.pdf>
- Compare AWS Support Plans:
<https://aws.amazon.com/premiumsupport/plans/>
- How AWS Pricing Works:
http://d1.awsstatic.com/whitepapers/aws_pricing_overview.pdf



© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

371

As part of your preparation for the AWS Certified Cloud Practitioner exam, we recommend that you review these technical papers and resources:

- Overview of Amazon Web Services: <https://d1.awsstatic.com/whitepapers/aws-overview.pdf>
- Compare AWS Support Plans: <https://aws.amazon.com/premiumsupport/plans>
- How AWS Pricing Works:
http://d1.awsstatic.com/whitepapers/aws_pricing_overview.pdf

Links to these papers and resources are included in the Additional Resources guide for this course.

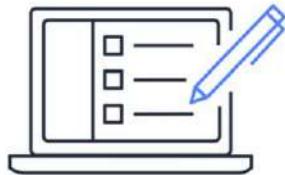
Exam strategies

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.



This section explores strategies that can help you pass the exam.

1. Read the full question.
2. Predict the answer before looking at the response options.
3. Exclude incorrect response options.



First, make sure that you read each question in full. Notice key words or phrases in a question that, if left unread, could result in you selecting an incorrect response option.

Next, try to predict the correct answer before looking at any of the response options. This strategy helps you to draw directly from your knowledge and skills without distraction from incorrect response options. If your prediction turns out to be one of the response options, this can be helpful for knowing whether you're on the right track. However, make sure that you review all the other response options for that question.

Before selecting your response to a question, eliminate any options that you believe are incorrect. This strategy helps you to focus on the correct option (or options, for multiple-response questions) and ensures that you have fulfilled all the requirements of the question.

Practice using these strategies in the following two sample questions. These questions will help you become familiar with the differences between multiple-choice and multiple-response questions.

Sample question 1 Multiple choice



374

AWS Certified Cloud Practitioner exam results are reported as a score from 100–1,000. What is the minimum passing score?

- A. 650
- B. 700
- C. 850
- D. 900

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Certified Cloud Practitioner exam results are reported as a score from 100–1,000. What is the minimum passing score?

- A. 650
- B. 700
- C. 850
- D. 900

Sample question 1 Multiple choice



375

AWS Certified Cloud Practitioner
exam results are reported as a score from 100–1,000. What is the **minimum** passing score?

- A. 650
- B. 700
- C. 850
- D. 900

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Key words and phrases that you might have identified in this question include **minimum** and **AWS Certified Cloud Practitioner**.

Sample question 1 Multiple choice



376

AWS Certified Cloud Practitioner
exam results are reported as a score from 100–1,000. What is the **minimum** passing score?

- A. 650
- B. 700 (correct)
- C. 850
- D. 900

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

After eliminating the incorrect response options, you can select the correct answer, which is **B. 700**.

Sample question 2 Multiple response



377

Which domains are included on the AWS Certified Cloud Practitioner exam? (Select TWO.)

- A. Security and Compliance
- B. Automation and Optimization
- C. Monitoring and Reporting
- D. Billing and Pricing
- E. Deployment and Provisioning

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Which domains are included on the AWS Certified Cloud Practitioner exam? (Select TWO.)

- A. Security and Compliance
- B. Automation and Optimization
- C. Monitoring and Reporting
- D. Billing and Pricing
- E. Deployment and Provisioning

Sample question 2 Multiple response



378

Which **domains** are included on the **AWS Certified Cloud Practitioner** exam? (Select TWO.)

- A. Security and Compliance
- B. Automation and Optimization
- C. Monitoring and Reporting
- D. Billing and Pricing
- E. Deployment and Provisioning

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Key words and phrases that you might have identified in this question include **domains** and **AWS Certified Cloud Practitioner**.

Strategy: Think back to the exam domains reviewed earlier. Based on the domains that you recall learning about, which response options can you reject as incorrect?

Sample question 2: Multiple response



379

Which **domains** are included on the **AWS Certified Cloud Practitioner** exam? (Select TWO.)

- A. **Security and Compliance (correct)**
- B. Automation and Optimization
- C. Monitoring and Reporting
- D. **Billing and Pricing (correct)**
- E. Deployment and Provisioning

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The two correct response options are:

- **A. Security and Compliance**
- **D. Billing and Pricing**

The other three response options are domains that are included on the AWS Certified SysOps Administrator – Associate exam.

As you continue to prepare for the AWS Certified Cloud Practitioner exam, review the sample exam questions and detailed answer explanations:

https://d1.awsstatic.com/training-and-certification/docs-cloud-practitioner/AWS-Certified-Cloud-Practitioner_Sample-Questions.pdf

End of course assessment



Complete the end of course assessment to review your understanding of AWS Cloud concepts:

AWS Partners:

<https://partnercentral.awspartner.com/LmsSsoRedirect?RelayState=%2flearningobject%2fwbc%3fid%3d70046>

In this course, you built your AWS Cloud knowledge by learning about AWS Cloud concepts, AWS services, security, architecture, pricing, and support. After taking the course, complete the following course assessment. A minimum score of 80 percent is required for course completion.

Access the end of course assessment at the following links:

AWS Partners:

<https://partnercentral.awspartner.com/APNLogin?startURL=%2FLmsSsoRedirect%3FRelayState%3D%252Flearningobject%252Fwbc%253Fid%253D66064>

Thank you

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited. Corrections, feedback, or other questions? Contact us at [AWS Feedback](#). All trademarks are the property of their owners.



Thank you for completing this course. Remember to review the additional resources and labs to learn more about AWS.

Also, please remember to complete the course assessment.