Module 1: Cloud Concepts Overview

Section 1: Introduction to cloud

computing

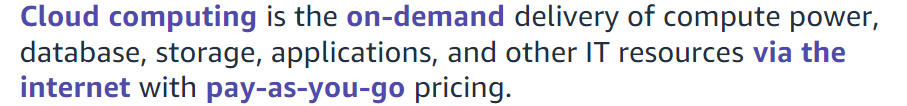
After completing this module, you should be able to:

• Define different types of cloud computing

• Describe six advantages of cloud computing

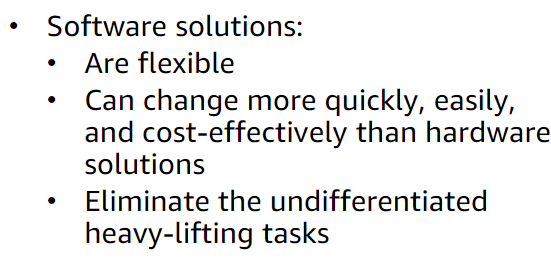
• Recognize the main AWS service categories and core services

• Review the AWS Cloud Adoption Framework (AWS CAF)

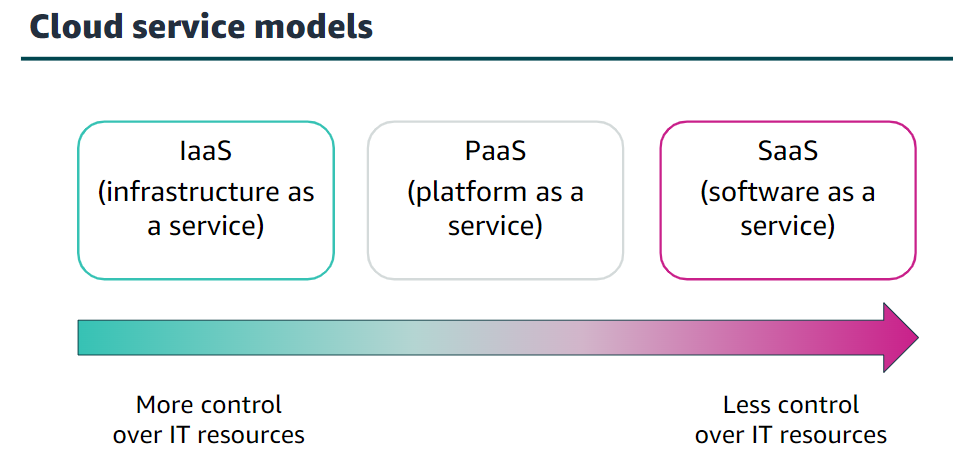


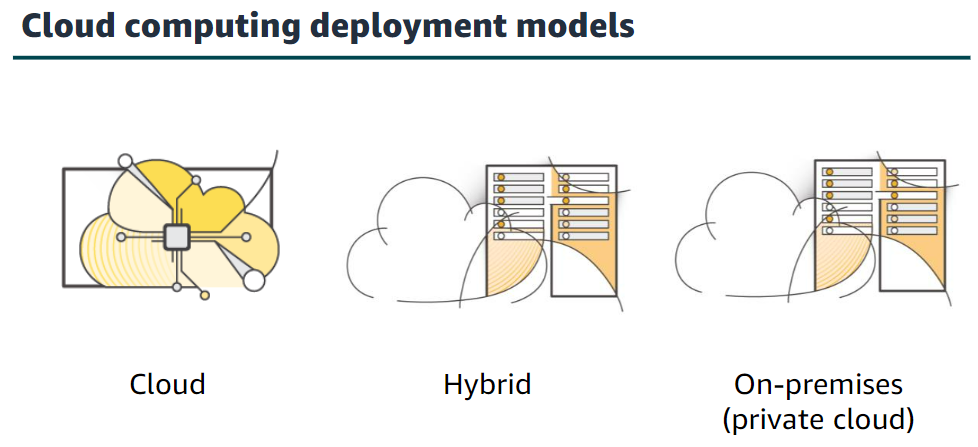
Cloud computing enables you to stop thinking of your infrastructure as hardware, and instead think of (and use) it as software.

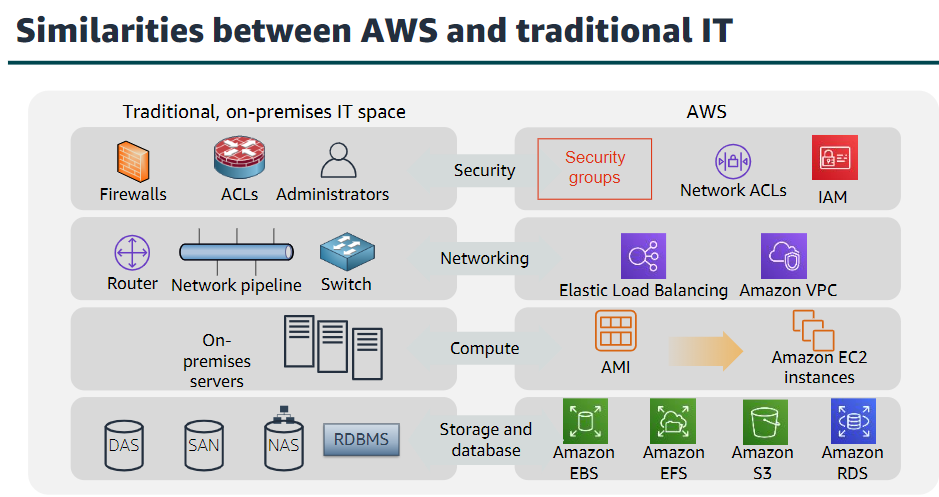
With a hardware solution, you must ask if there is enough resource capacity or sufficient storage to meet your needs, and you provision capacity by guessing theoretical maximum peaks. If you don’t meet your projected maximum peak, then you pay for expensive resources that stay idle. If you exceed your projected maximum peak, then you don’t have sufficient capacity to meet your needs. And if your needs change, then you must spend the time, effort, and money required to implement a new solution.



Cloud computing helps developers and IT departments avoid undifferentiated work like procurement, maintenance, and capacity planning, thus enabling them to focus on what matters most.

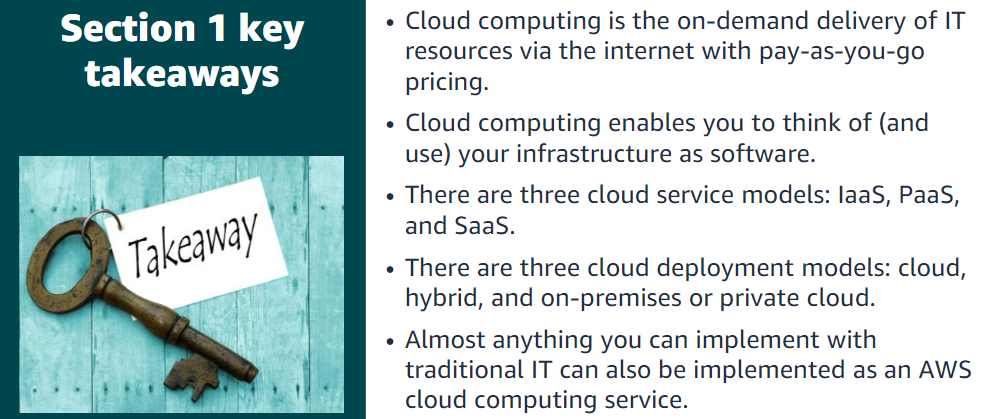


* Infrastructure as a service (IaaS): Services in this category are the basic building blocks for cloud IT and typically provide you with access to networking features, computers (virtual or on dedicated hardware), and data storage space.
* Platform as a service (PaaS): Services in this category reduce the need for you to manage the underlying infrastructure (usually hardware and operating systems) and enable you to focus on the deployment and management of your applications.
* Software as a service (SaaS): Services in this category provide you with a completed product that the service provider runs and manages. In most cases, software as a service refers to end-user applications. With a SaaS offering, you do not have to think about how the service is maintained or how the underlying infrastructure is managed   
    
  
* Cloud: A cloud-based application is fully deployed in the cloud, and all parts of the application run in the cloud. Applications in the cloud have either been created in the cloud or have been migrated from an existing infrastructure to take advantage of the benefits of cloud computing
* Hybrid: The most common method of hybrid deployment is between the cloud and existing on-premises infrastructure. This model enables an organization to extend and grow their infrastructure into the cloud while connecting cloud resources to internal systems.
* On-premises: Deploying resources on-premises, using virtualization and resource management tools, is sometimes called private cloud. While on-premises deployment does not provide many of the benefits of cloud computing, it is sometimes sought for its ability to provide dedicated resources.



There are many similarities between AWS and the traditional, on-premises IT space:

* AWS security groups, network access control lists (network ACLs), and AWS Identity and Access Management (IAM) are similar to firewalls, access control lists (ACLs), and administrators.
* Elastic Load Balancing and Amazon Virtual Private Cloud (Amazon VPC) are similar to routers, network pipelines, and switches.
* Amazon Machine Images (AMIs) and Amazon Elastic Compute Cloud (Amazon EC2) instances are similar to on-premises servers.
* Amazon Elastic Block Store (Amazon EBS), Amazon Elastic File System (Amazon EFS), Amazon Simple Storage Service (Amazon S3), and Amazon Relational Database Service (Amazon RDS) are similar to direct attached storage (DAS), storage area networks (SAN), network attached storage (NAS), and a relational database management service (RDBMS).



Section 2: Advantages of cloud

computing

Advantage #1—Trade capital expense for variable expense: Capital expenses (capex) are funds that a company uses to acquire, upgrade, and maintain physical assets such as property, industrial buildings, or equipment.

By contrast, a variable expense is an expense that the person who bears the cost can easily alter or avoid. Instead of investing heavily in data centers and servers before you know how you will use them, you can pay only when you consume resources and pay only for the amount you consume. Thus, you save money on technology.

Advantage #2—Benefit from massive economies of scale: By using cloud computing, you can achieve a lower variable cost than you can get on your own. Because usage from hundreds of thousands of customers is aggregated in the cloud, providers such as AWS can achieve higher economies of scale, which translates into lower pay-as-you-go prices.

Advantage #3—Stop guessing capacity: Eliminate guessing about your infrastructure capacity needs. When you make a capacity decision before you deploy an application, you often either have expensive idle resources or deal with limited capacity. With cloud computing, these problems go away.

Advantage #4—Increase speed and agility: In a cloud computing environment, new IT resources are only a click away, which means that you reduce the time it takes to make those resources available to your developers from weeks to just minutes.

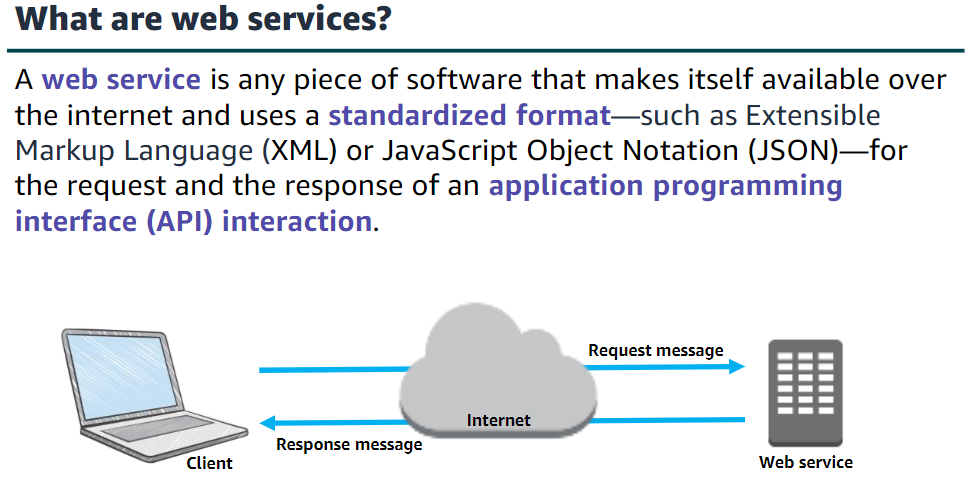
Advantage #5—Stop spending money on running and maintaining data centres: Focus on projects that differentiate your business instead of focusing on the infrastructure.

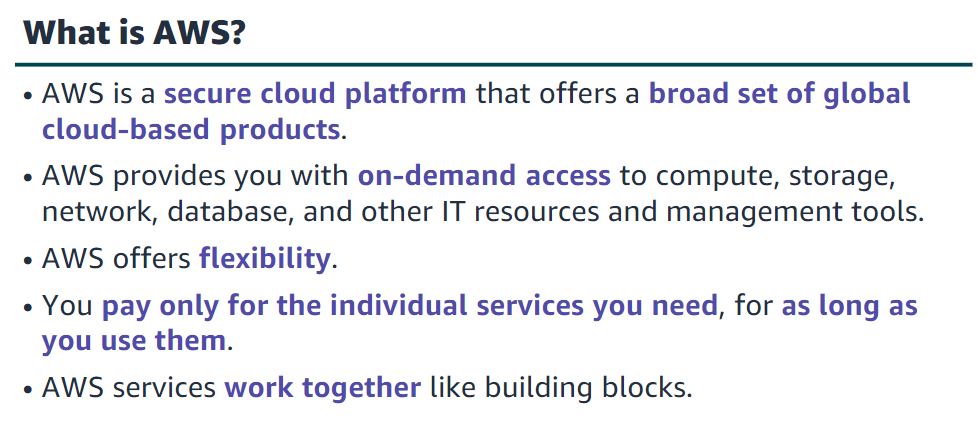
Advantage #6—Go global in minutes: You can deploy your application in multiple AWS Regions around the world with just a few clicks. As a result, you can provide a lower latency and better experience for your customers simply and at minimal cost

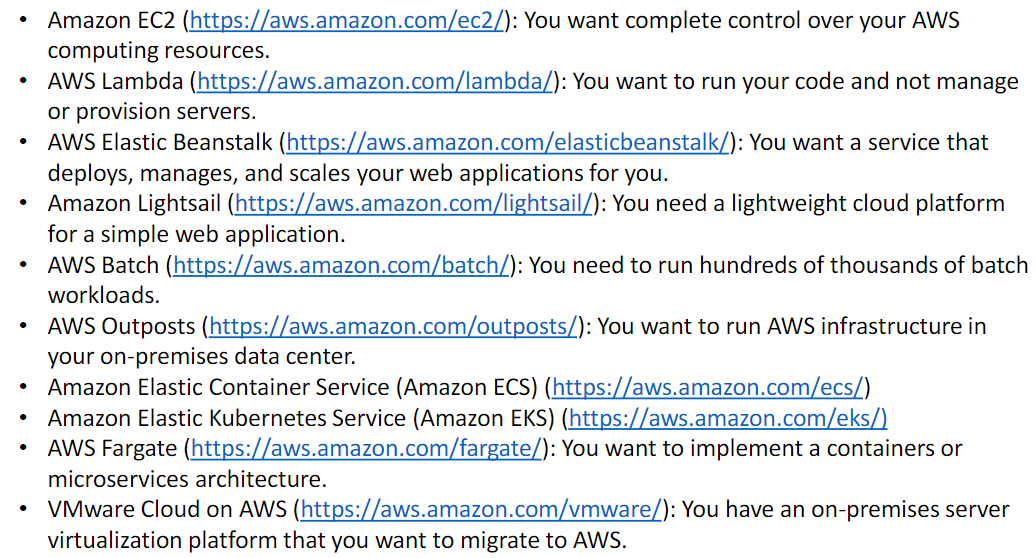


Section 3: Introduction to Amazon

Web Services (AWS)





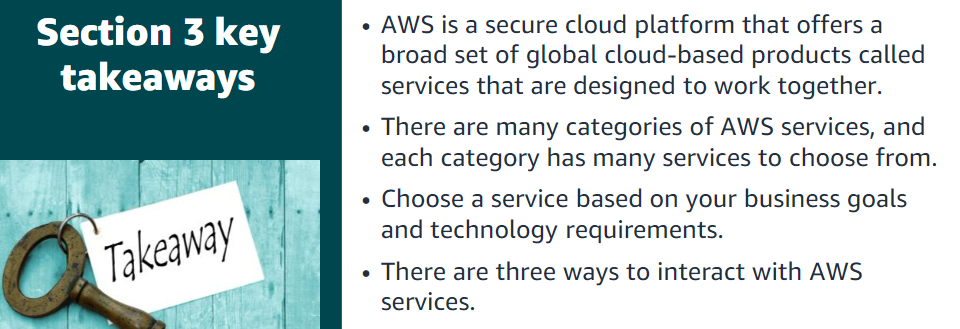


There are three ways to create and manage resources on the AWS Cloud:

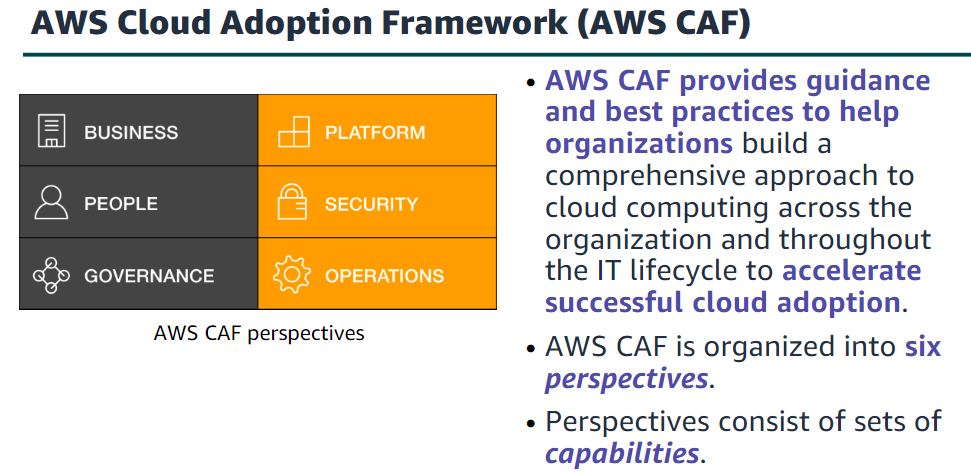
**•AWS Management Console**: The console provides a rich graphical interface to a majority of the features offered by AWS.

**•AWS Command Line Interface (AWS CLI):** The AWS CLI provides a suite of utilities that can be launched from a command script in Linux, macOS, or Microsoft Windows.

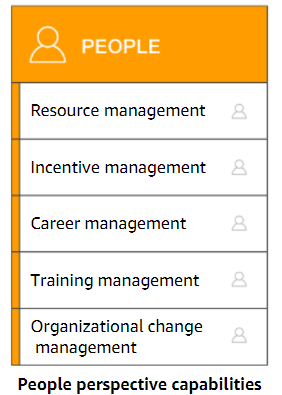
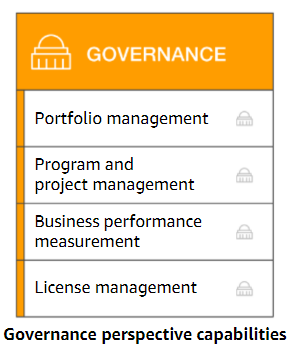
**•Software development kits (SDKs):** AWS provides packages that enable accessing AWS in a variety of popular programming languages.

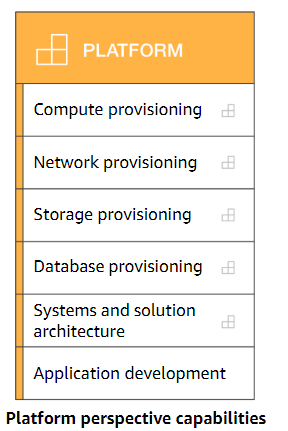


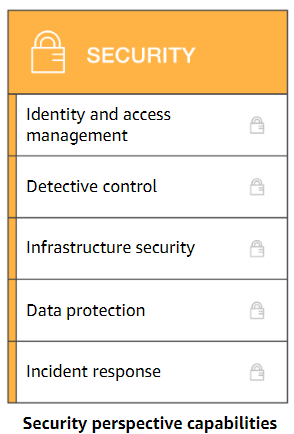
Section 4: Moving to the AWS Cloud –The AWS Cloud Adoption Framework (AWS CAF)



Business V/S Technical

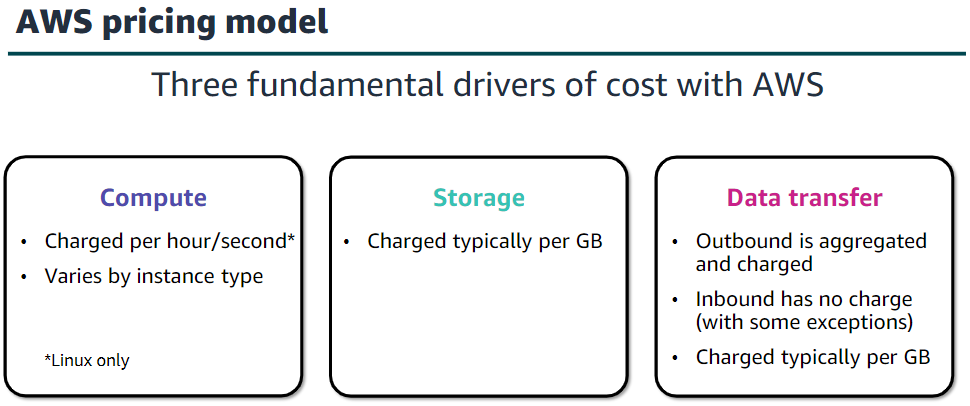






Module 2: Cloud Economics and Billing

Section 1: Fundamentals of pricing



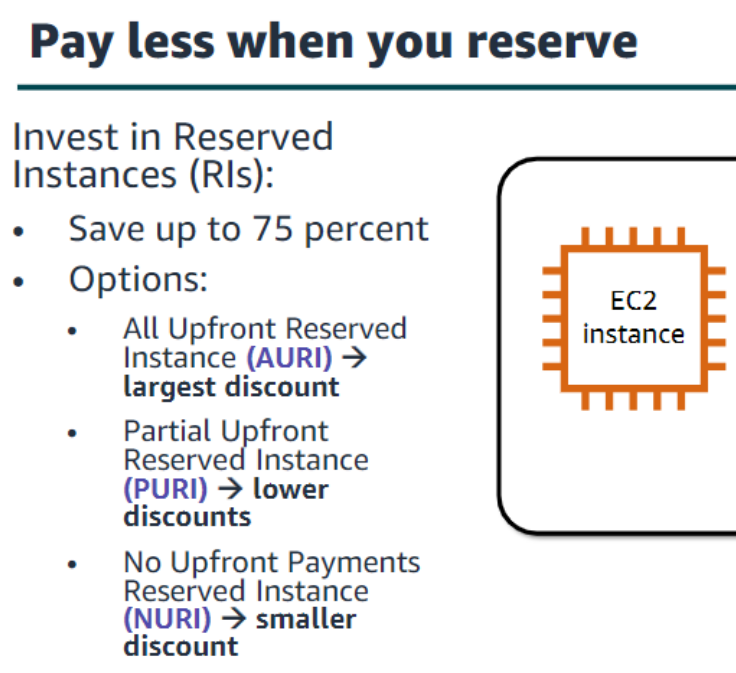
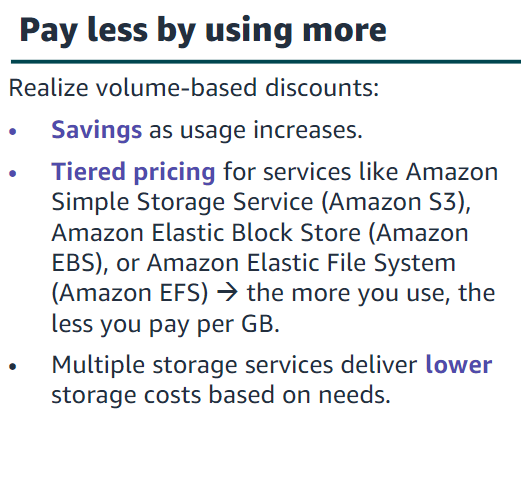
AWS offers a range of cloud computing services. For each service, you pay for exactly the amount of resources that you actually need. This utility-style pricing model includes:

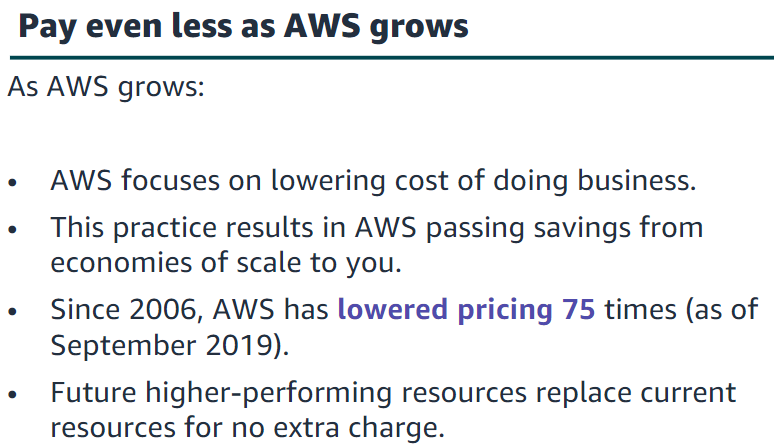
•Pay for what you use

•Pay less when you reserve

•Pay less when you use more

•Pay even less as AWS grows







•Amazon Virtual Private Cloud (Amazon VPC) enables you to provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define.

•AWS Identity and Access Management (IAM) controls your users’ access to AWS services and resources.

•Consolidated Billing is a billing feature in AWS Organizations to consolidate payment for multiple AWS accounts or multiple Amazon Internet Services Private Limited (AISPL) accounts\*.

Consolidated billing provides:

•One bill for multiple accounts.

•The ability to easily track each account’s charges.

•The opportunity to decrease charges as a result of volume pricing discounts from

combined usage.

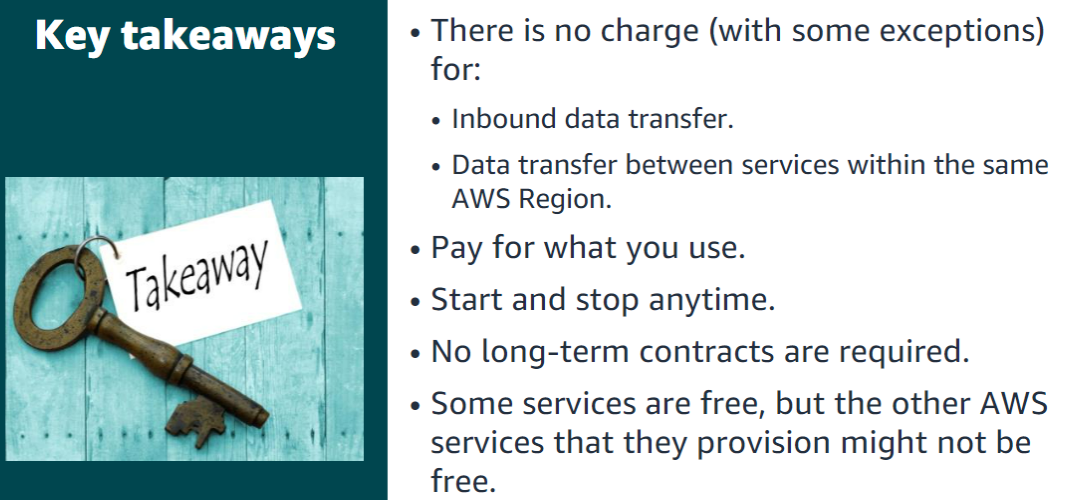
•And you can consolidate all of your accounts using Consolidated Billing and get tiered benefits.

•AWS Elastic Beanstalk is an even easier way for you to quickly deploy and manage applications in the AWS Cloud.

• AWS CloudFormation gives developers and systems administrators an easy way to create a collection of related AWS resources and provision them in an orderly and predictable fashion.

•Automatic Scaling automatically adds or removes resources according to conditions you define. The resources you are using increase seamlessly during demand spikes to maintain performance and decrease automatically during demand lulls to minimize costs.

•AWS OpsWorks is an application management service that makes it easy to deploy and operate applications of all shapes and sizes.



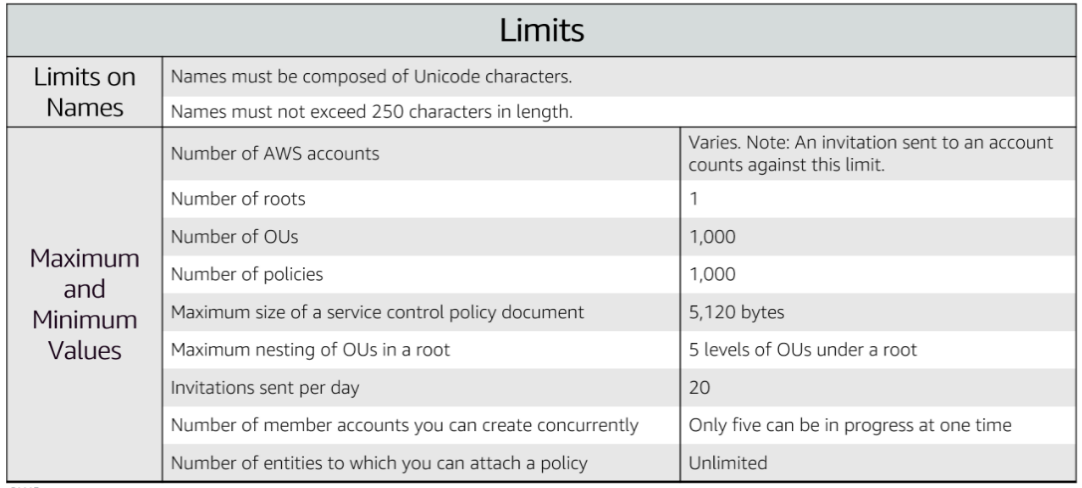
Section 2: Total Cost of Ownership

Total Cost of Ownership (TCO) is the financial estimate to help identify direct and indirect costs of a system

Some of the costs that are associated with data center management include: •Server costs for both hardware and software, and facilities costs to house the equipment.   
•Storage costs for the hardware, administration, and facilities.   
•Network costs for hardware, administration, and facilities.   
•And IT labour costs that are required to administer the entire solution.

Section 3: AWS Organizations

AWS Organizations is a free account management service that enables you to consolidate multiple AWS accounts into an organization that you create and centrally manage.



AWS Organizations can be managed through different interfaces.

The AWS Management Console is a browser-based interface that you can use to manage your organization and your AWS resources. You can perform any task in your organization by using the console.

AWS Command Line Interface(AWS CLI) tools enable you to issue commands at your system's command line to perform AWS Organizations tasks and AWS tasks. This method can be faster and more convenient than using the console.

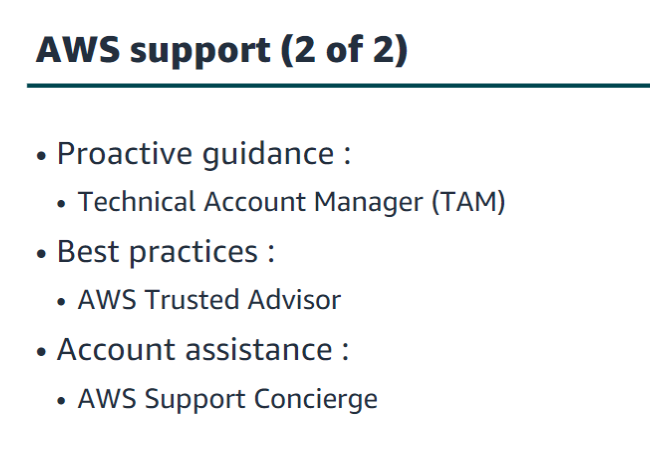
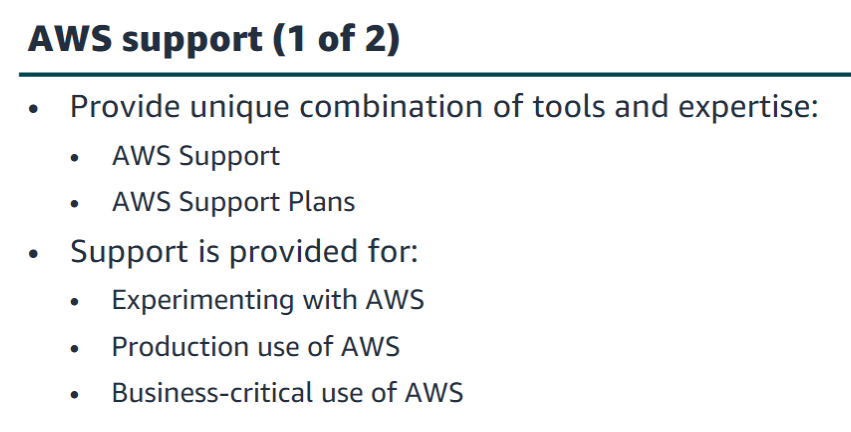
You can use also AWS software development kits (SDKs) to handle tasks such as cryptographically signing requests, managing errors, and retrying requests automatically. AWS SDKs consist of libraries and sample code for various programming languages and platforms, such as Java, Python, Ruby, .NET, iOS, and Android.

The AWS Organizations HTTPS Query API gives you programmatic access to AWS Organizations and AWS. You can use the API to issue HTTPS requests directly to the service. When you use the HTTPS API, you must include code to digitally sign requests by using your credentials.

Section 4: AWS Billing and Cost Management

AWS Billing and Cost Management is the service that you use to pay your AWS bill, monitor your usage, and budget your costs.  
The AWS Cost and Usage Report Tool enables you to identify opportunities for optimization by understanding your cost and usage data trends and how you are using your AWS implementation.  
The AWS Billing Dashboard lets you view the status of your month-to-date AWS expenditure, identify the services that account for the majority of your overall expenditure, and understand at a high level how costs are trending.  
The AWS Bills page lists the costs that you incurred over the past month for each AWS service, with a further breakdown by AWS Region and linked account.  
The AWS Billing and Cost Management console includes the Cost Explorer page for viewing your AWS cost data as a graph.  
AWS Budgets uses the cost visualization that is provided by Cost Explorer to show you the status of your budgets and to provide forecasts of your estimated costs.  
Budget alerts can be sent via email or via Amazon Simple Notification Service (Amazon SNS).

Section 5: Technical support



The Basic Support Plan offers:  
•24/7 access to customer service, documentation, whitepapers and support forums.  
•Access to six core Trusted Advisor checks.  
•Access to Personal Health Dashboard.

•The Developer Support Plan offers resources for customers that are testing or doing early development on AWS, and any customers who:  
•Want access to guidance and technical support.  
•Are exploring how to quickly put AWS to work.  
•Use AWS for non-production workloads or applications.

The Business Support Plan offers resources for customers that are running production workloads on AWS and any customers who:  
•Run one or more applications in production environments.  
•Have multiple services activated, or use key services extensively.  
•Depend on their business solutions to be available, scalable, and secure.

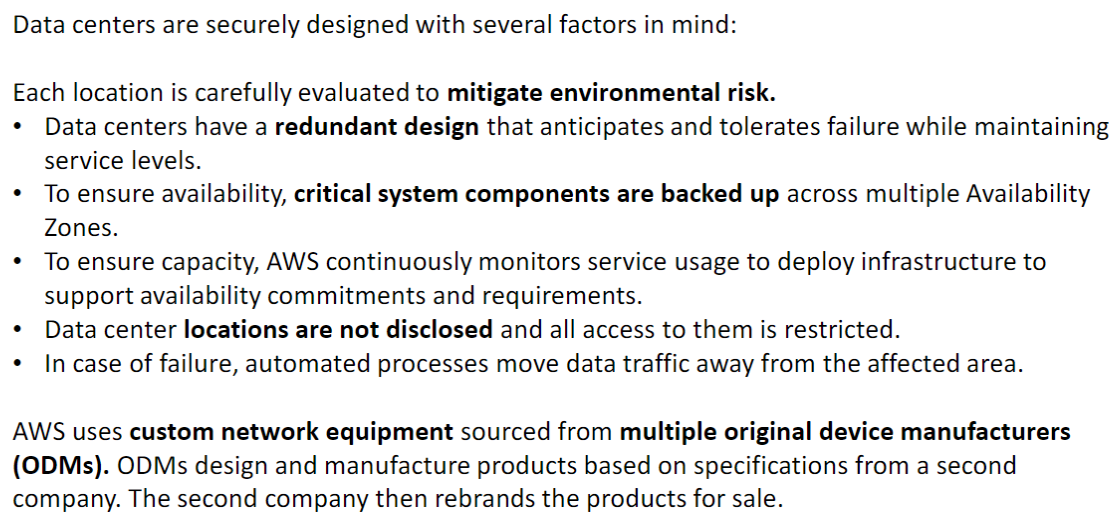
There are five different severity levels:

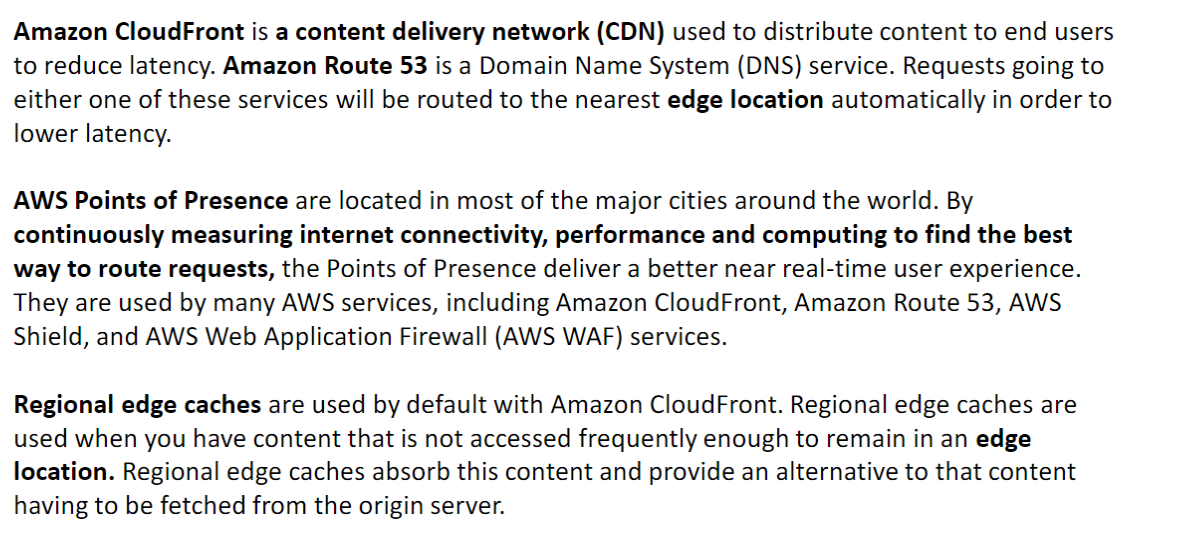
•Critical–Your business is at risk. Critical functions of your application are unavailable.  
•Urgent–Your business is significantly impacted. Important functions of your application are unavailable.  
•High–Important functions of your application are impaired or degraded.  
•Normal–Non-critical functions of your application are behaving abnormally, or you have a time-sensitive development question.  
•Low–You have a general development question, or you want to request a feature.

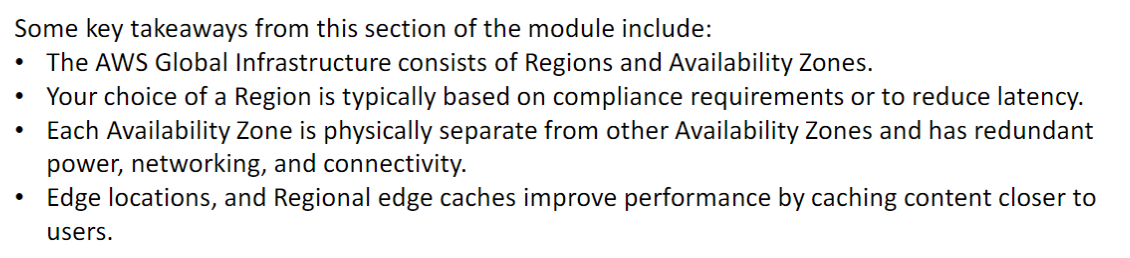
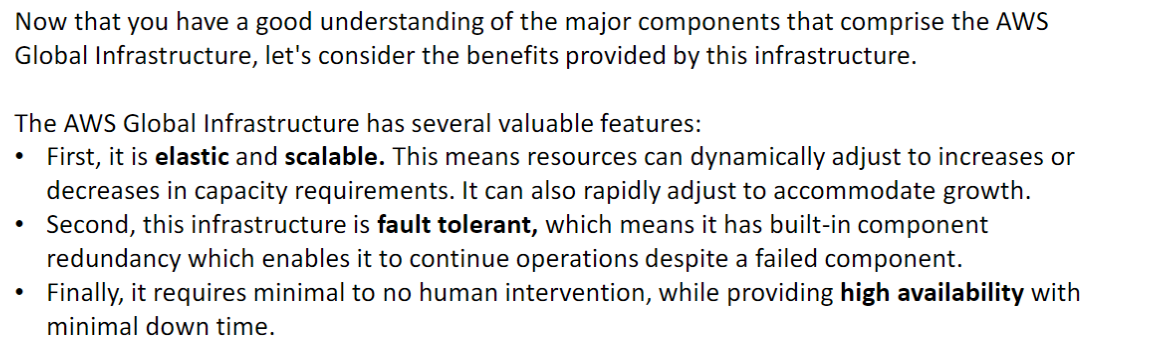
Module 3: AWS Global Infrastructure Overview

Section 1: AWS Global Infrastructure

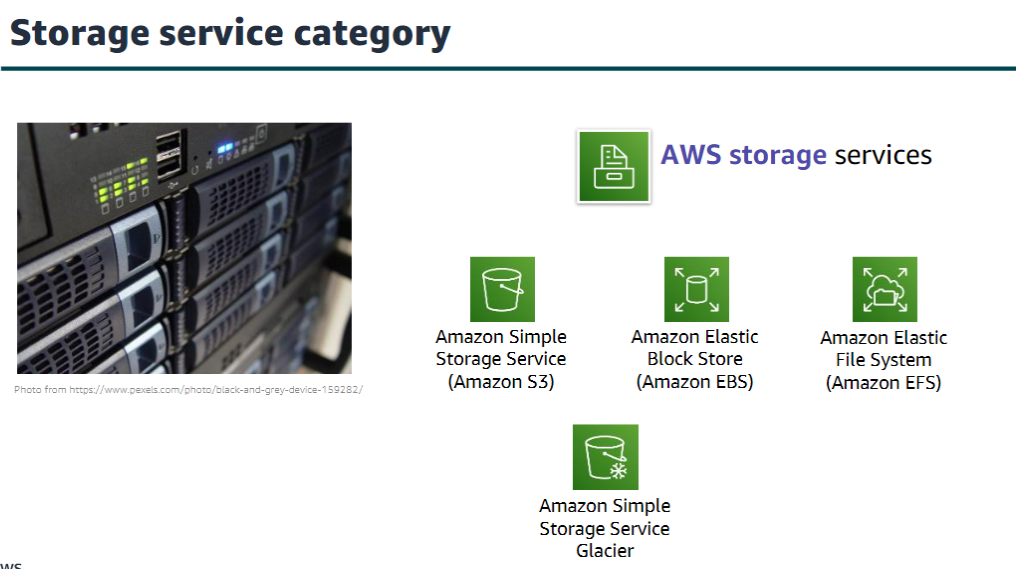
The AWS Cloud infrastructure is built around Regions.   
AWS has 22 Regions worldwide. An AWS Region is a physical geographical location with one or more Availability Zones. Availability Zones in turn consist of one or more data centers.  
To achieve fault tolerance and stability, Regions are isolated from one another. Resources in one Region are not automatically replicated to other Regions. When you store data in a specific Region, it is not replicated outside that Region. It is your responsibility to replicate data across Regions, if your business needs require it.   
AWS Regions that were introduced before March 20, 2019 are enabled by default. Regions that were introduced after March 20, 2019—such as Asia Pacific (Hong Kong) and Middle East (Bahrain)—are disabled by default. You must enable these Regions before you can use them. You can use the AWS Management Console to enable or disable a Region. Some Regions have restricted access. An Amazon AWS (China) account provides access to the Beijing and Ningxia Regions only.   
To learn more about AWS in China, see: https://www.amazonaws.cn/en/about-aws/china/. The isolated AWS GovCloud (US) Region is designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements.   
For accessibility: Snapshot from the infrastructure. AWS website that shows a picture of downtown London including the Tower Bridge and the Shard. It notes that there are three Availability Zones in the London region. End of accessibility description.







Section 2: AWS services and service category overview

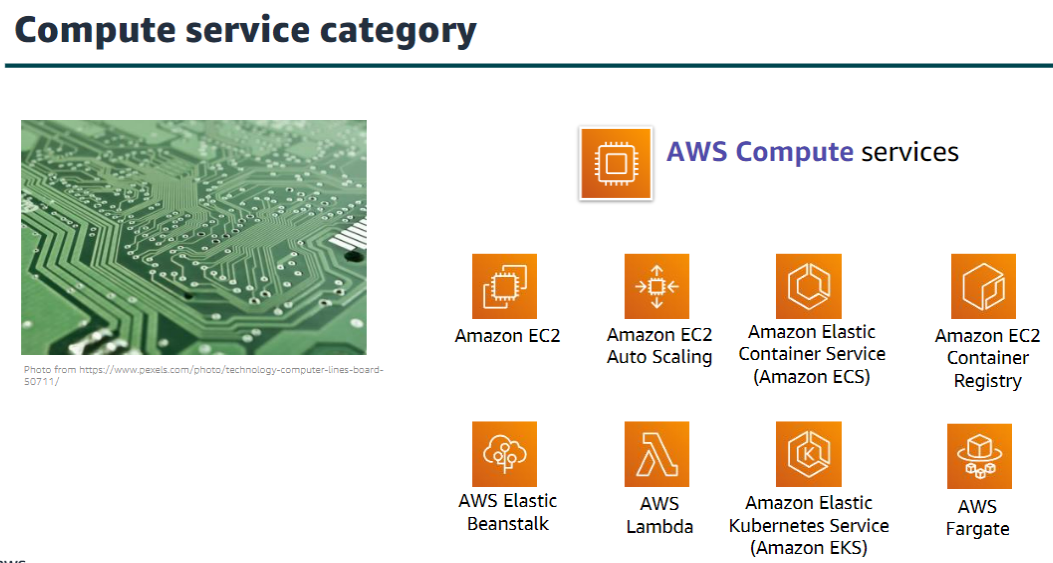


Amazon Simple Storage Service (Amazon S3) is an object storage service that offers scalability, data availability, security, and performance. Use it to store and protect any amount of data for websites, mobile apps, backup and restore, archive, enterprise applications, Internet of Things (IoT) devices, and big data analytics.

Amazon Elastic Block Store (Amazon EBS) is high-performance block storage that is designed for use with Amazon EC2 for both throughput and transaction-intensive workloads. It is used for a broad range of workloads, such as relational and non-relational databases, enterprise applications, containerized applications, big data analytics engines, file systems, and media workflows.

Amazon Elastic File System (Amazon EFS) provides a scalable, fully managed elastic Network File System (NFS) file system for use with AWS Cloud services and on-premises resources. It is built to scale on demand to petabytes, growing and shrinking automatically as you add and remove files. It reduces the need to provision and manage capacity to accommodate growth.

Amazon Simple Storage Service Glacier is a secure, durable, and extremely low-cost Amazon S3 cloud storage class for data archiving and long-term backup. It is designed to deliver 11 9s of durability and to provide comprehensive security and compliance capabilities to meet stringent regulatory requirements.



AWS compute services include the services listed here, and many others.   
  
Amazon Elastic Compute Cloud (Amazon EC2) provides resizable compute capacity as virtual machines in the cloud. Amazon EC2 Auto Scaling enables you to automatically add or remove EC2 instances according to conditions that you define.

Amazon Elastic Container Service (Amazon ECS) is a highly scalable, high-performance container orchestration service that supports Docker containers.

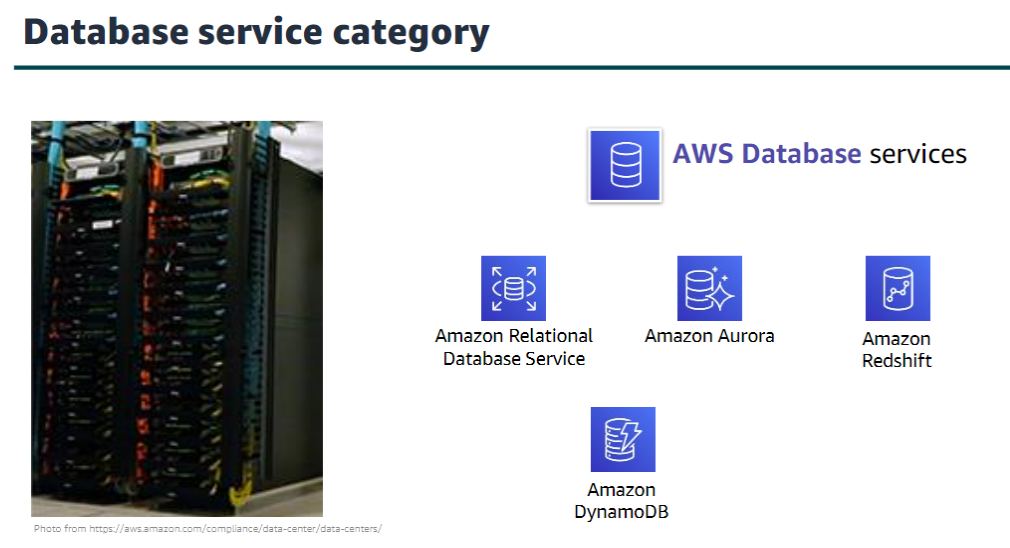
Amazon Elastic Container Registry (Amazon ECR) is a fully-managed Docker container registry that makes it easy for developers to store, manage, and deploy Docker container images.

AWS Elastic Beanstalk is a service for deploying and scaling web applications and services on familiar servers such as Apache and Microsoft Internet Information Services (IIS).

AWS Lambda enables you to run code without provisioning or managing servers. You pay only for the compute time that you consume. There is no charge when your code is not running.

Amazon Elastic Kubernetes Service (Amazon EKS) makes it easy to deploy, manage, and scale containerized applications that use Kubernetes on AWS.

AWS Fargate is a compute engine for Amazon ECS that allows you to run containers without having to manage servers or clusters.



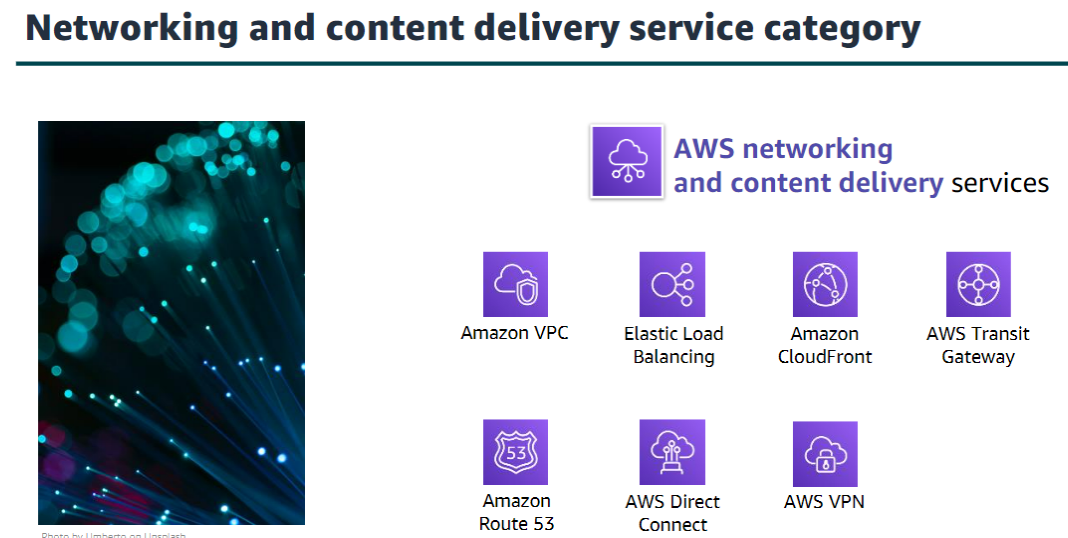
AWS database services include the services listed here, and many others.

Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud.   
It provides resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching, and backups.

Amazon Aurora is a MySQL and PostgreSQL-compatible relational database.   
It is up to five times faster than standard MySQLdatabases and three times faster than standard PostgreSQL databases.

Amazon Redshift enables you to run analytic queries against petabytes of data that is stored locally in Amazon Redshift, and directly against exabytes of data that are stored in Amazon S3. It delivers fast performance at any scale.

Amazon DynamoDB is a key-value and document database that delivers single-digit millisecond performance at any scale, with built-in security, backup and restore, and in-memory caching



Amazon Virtual Private Cloud (Amazon VPC) enables you to provision logically isolated sections of the AWS Cloud.

Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions.

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and application programming interfaces (APIs) to customers globally, with low latency and high transfer speeds.

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

Amazon Route 53 is a scalable cloud Domain Name System (DNS) web service designed to give you a reliable way to route end users to internet applications. It translates names (like www.example.com) into the numeric IP addresses (like 192.0.2.1) that computers use to connect to each other.

AWS Direct Connect provides a way to establish a dedicated private network connection from your data center or office to AWS, which can reduce network costs and increase bandwidth throughput.

AWS VPN provides a secure private tunnel from your network or device to the AWS global network.



AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. By using IAM, you can create and manage AWS users and groups. You can use IAM permissions to allow and deny user and group access to AWS resources.

AWS Organizations allows you to restrict what services and actions are allowed in your accounts.

Amazon Cognito lets you add user sign-up, sign-in, and access control to your web and mobile apps.

AWS Artifact provides on-demand access to AWS security and compliance reports and select online agreements.

AWS Key Management Service (AWS KMS) enables you to create and manage keys. You can use AWS KMS to control the use of encryption across a wide range of AWS services and in your applications.

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



The AWS Cost and Usage Report contains the most comprehensive set of AWS cost and usage data available, including additional metadata about AWS services, pricing, and reservations.

AWS Budgets enables you to set custom budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budgeted amount.

AWS Cost Explorer has an easy-to-use interface that enables you to visualize, understand, and manage your AWS costs and usage over time.



The AWS Management Console provides a web-based user interface for accessing your AWS account.

AWS Config provides a service that helps you track resource inventory and changes.

Amazon CloudWatch allows you to monitor resources and applications.

AWS Auto Scaling provides features that allow you to scale multiple resources to meet demand.

AWS Command Line Interface provides a unified tool to manage AWS services.

AWS Trusted Advisor helps you optimize performance and security.

AWS Well-Architected Tool provides help in reviewing and improving your workloads.

AWS CloudTrail tracks user activity and API usage.

Module 4: AWS Cloud Security

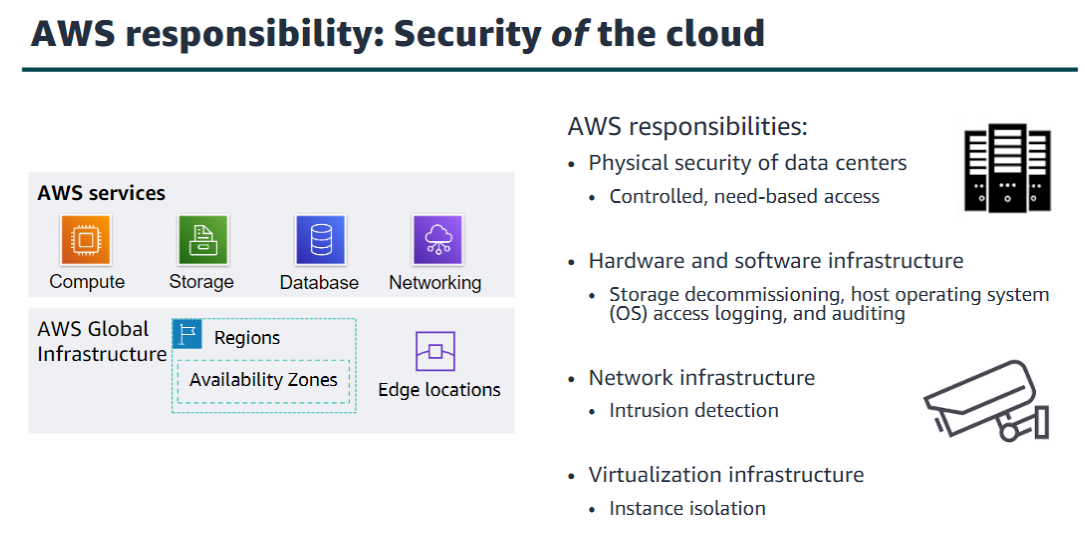
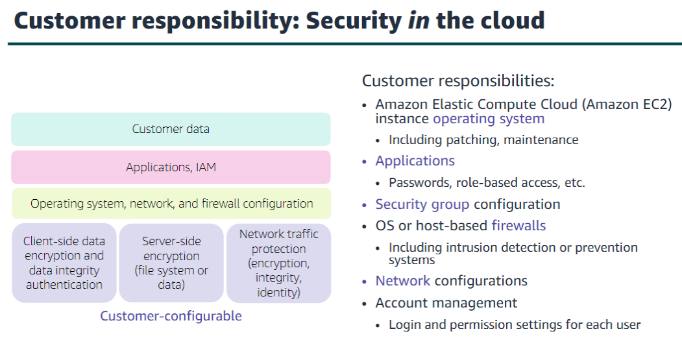
Section 1: AWS shared

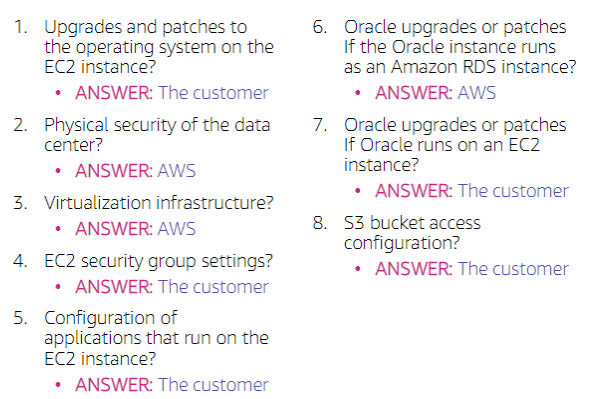
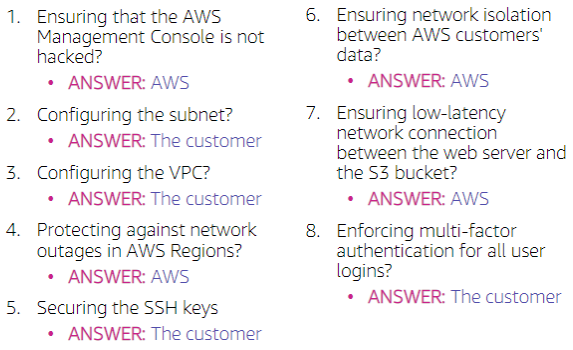
responsibility model

The differentiation of who is responsible for what is commonly referred to as security “of” the cloud versus security “in” the cloud.

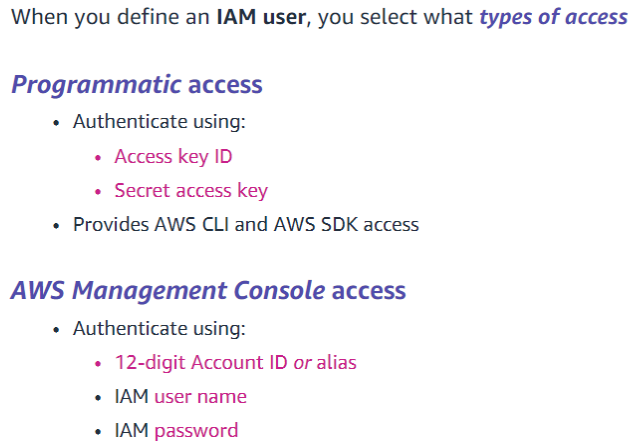
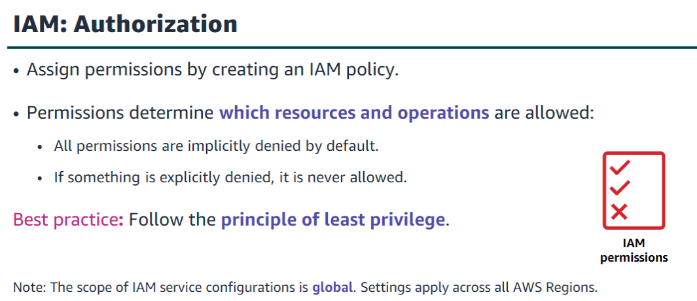
AWS operates, manages, and controls the components from the software virtualization layer down to the physical security of the facilities where AWS services operate. AWS is responsible for protecting the infrastructure that runs all the services that are offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run the AWS Cloud services.

The customer is responsible for the encryption of data at rest and data in transit. The customer should also ensure that the network is configured for security and that security credentials and logins are managed safely. Additionally, the customer is responsible for the configuration of security groups and the configuration of the operating system that run on compute instances that they launch (including updates and security patches.





Section 2: AWS Identity and Access Management (IAM)



An explicit deny statement takes precedence over an allow statement.

Resource-based policies are defined inline only, which means that you define the policy on the resource itself, instead of creating a separate IAM policy document that you attach.

An IAM Group is a collection of IAM users. IAM groups offer a convenient way to specify permissions for a collection of users, which can make it easier to manage the permissions for those users.

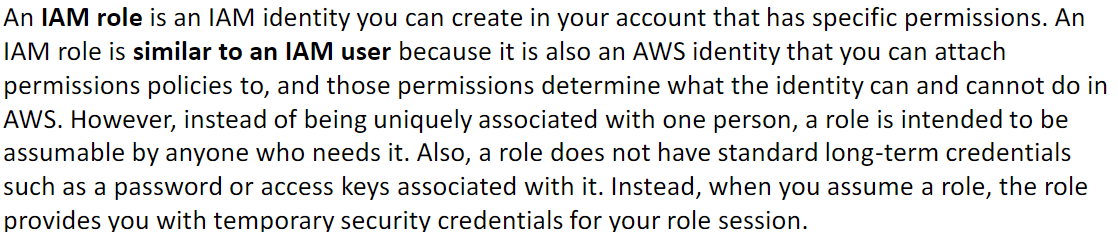
Important characteristics of IAM groups:

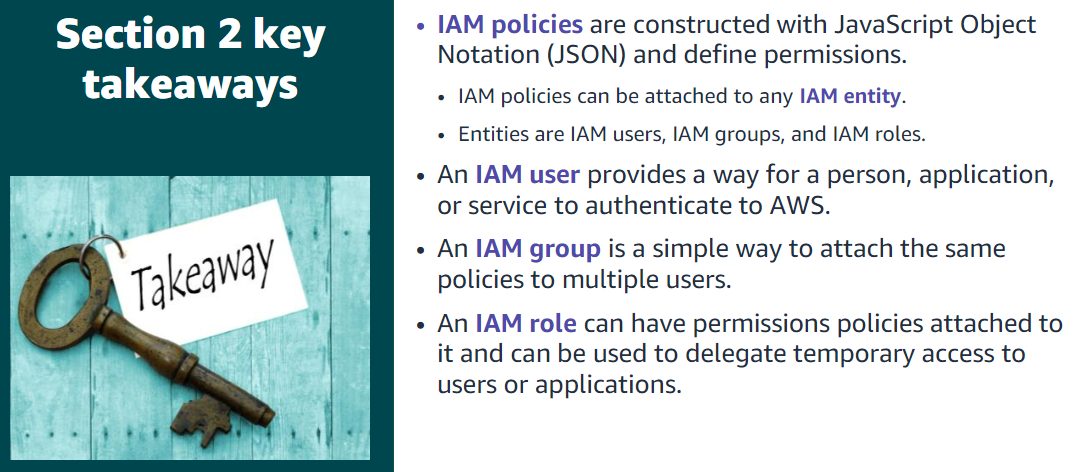
• A group can contain many users, and a user can belong to multiple groups.

• Groups cannot be nested. So a group can contain only users, and a group cannot contain other groups.

• There is no default group that automatically includes all users in the AWS account. If you want

to have a group with all account users in it, you need to create the group and add each new user to it.



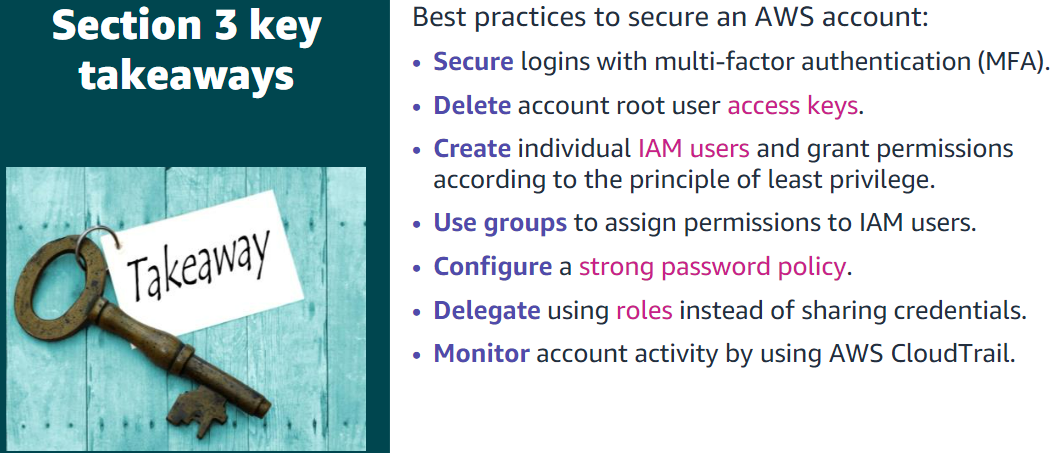


Section 3: Securing a new AWS account



AWS CloudTrail is enabled on account creation by default on all AWS accounts, and it keeps a record of the last 90 days of account management event activity.

You can view and download the last 90 days of your account activity for creating, modifying, and deleting related operations of services that are supported by CloudTrail without needing to manually create another trail.



Section 4: Securing accounts

AWS Organizations is an account management service that enables you to consolidate multiple AWS accounts into an organization that you create and centrally manage. Here, the focus is on the security features that AWS Organizations provides. One helpful security feature is that you can group accounts into organizational units(OUs) and attach different access policies to each OU.

Another security feature is that AWS organizations integrate with and supports IAM. AWS Organizations expands that control to the account level by giving you control over what users and roles in an account or a group of accounts can do.

Finally, AWS Organizations provides service control policies (SCPs) that enable you to specify the maximum permissions that member accounts in the organization can have. In SCPs, you can restrict which AWS services, resources, and individual actions the users and roles in each member account can access. These restrictions even override the administrators of member accounts. When AWS Organizations blocks access to a service, resource, or API action, a user or role in that account can't access it, even if an administrator of a member account explicitly grants such permissions.

SCPs are similar to IAM permissions policies – •They use similar syntax.

•However, an SCP never grants permissions.

•Instead, SCPs specify the maximum permissions for an organization.

