ITCS 443 Parallel and Distributed Systems

Introduction to AWS and AWS Security

aws academy

Agenda

- Introduction to AWS
  - What is AWS and their service category overview
  - Fundamentals of pricing and technical supports
  - AWS organizations
  - AWS global infrastructure
- Introduction to AWS cloud security
  - AWS shared responsibility model
  - AWS identity and access management (IAM)
  - Security a new AWS account
  - Securing accounts and data on AWS

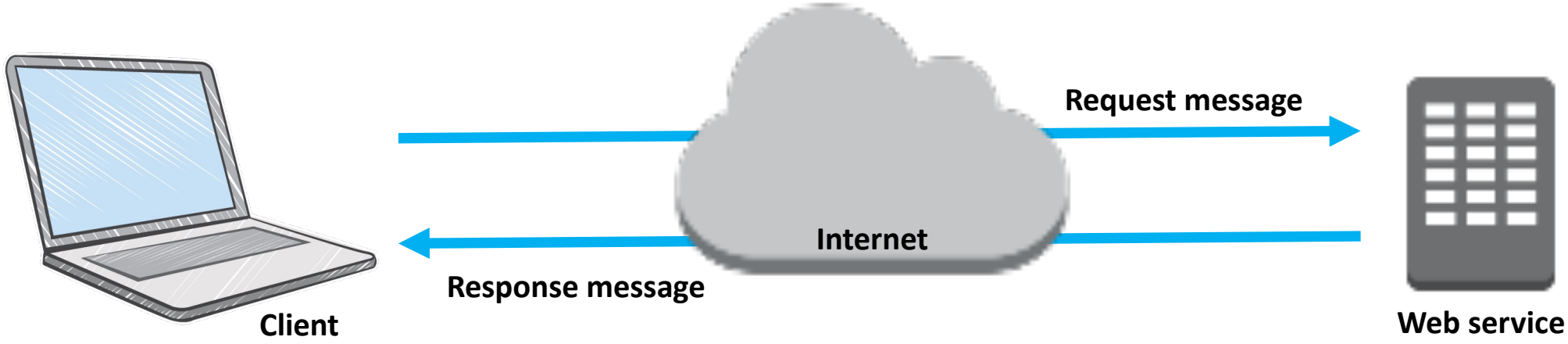
Introduction to AWS

Introduction to AWS and Service Category Overview

aws academy

What are web services?

A **web service** is any piece of software that makes itself available over the internet and uses a **standardized format**—such as Extensible Markup Language (XML) or JavaScript Object Notation (JSON)—for the request and the response of an **application programming interface (API) interaction**.



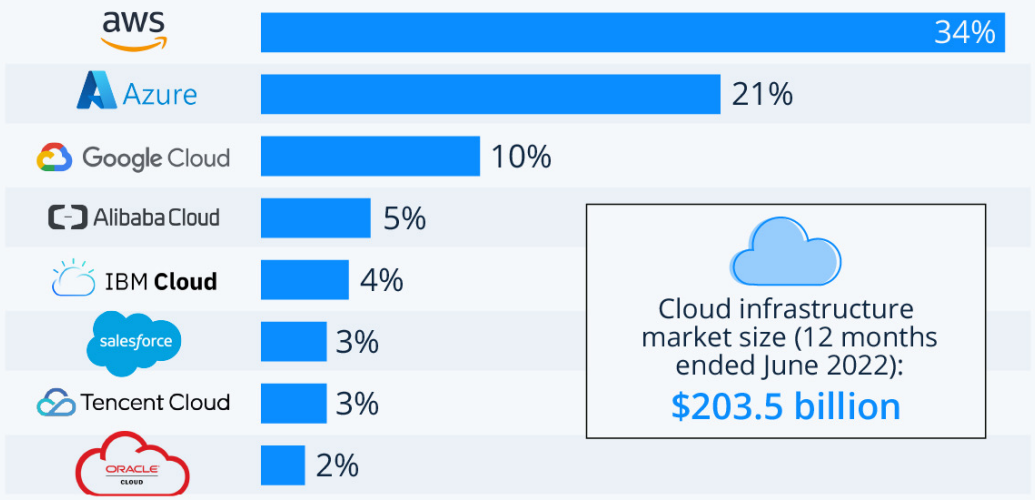
What is AWS?

- AWS is a **secure cloud platform** that offers a **broad set of global cloud-based products**.
- AWS provides you with **on-demand access** to compute, storage, network, database, and other IT resources and management tools.
- AWS offers **flexibility**.
- You **pay only for the individual services you need**, for **as long as you use them**.
- AWS services **work together** like building blocks.

Cloud Market

Amazon Leads $200-Billion Cloud Market

Worldwide market share of leading cloud infrastructure service providers in Q2 2022*



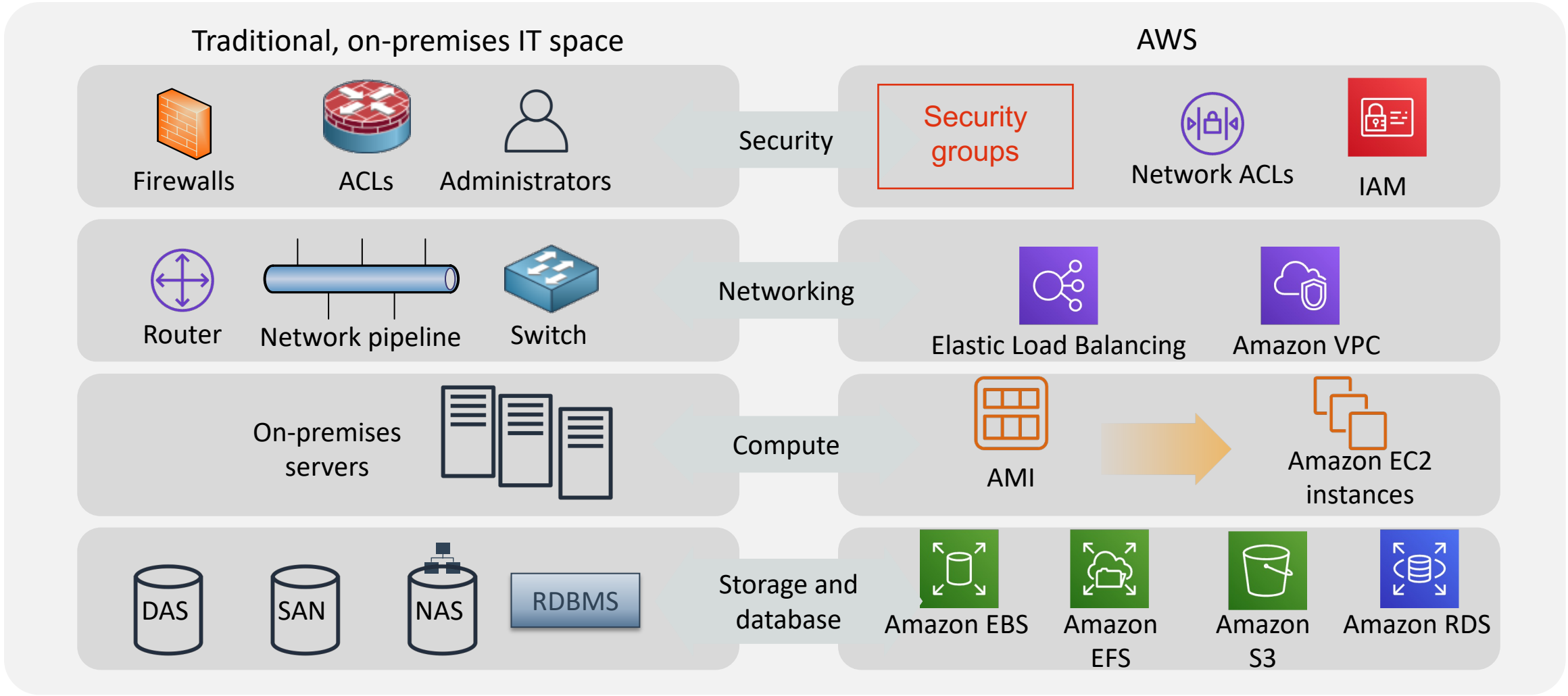
* includes platform as a service (PaaS) and infrastructure as a service (IaaS) as well as hosted private cloud services

Source: Synergy Research Group

statista

Figure 1: Magic Quadrant for Cloud Infrastructure and Platform Services

Similarities between AWS and traditional IT



AWS foundational services

Applications

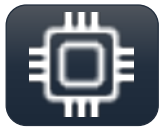
 Virtual desktops

 Collaboration and sharing

Platform Services

Databases	Analytics	Application services	Deployment and management	Mobile Services
Relational	Cluster computing	Queuing	Containers	Identity
NoSQL	Real-time	Orchestration	DevOps tools	Sync
Caching	Data warehouse	App Streaming	Resource templates	Mobile Analytics
	Data workflows	Transcoding	Usage tracking	Notifications
		Email	Monitoring and logs	
		Search		

Foundation Services

 Compute (virtual, automatic scaling, and load balancing)

 Networking

 Storage (object, block, and archive)

Infrastructure

Regions

Availability Zones

 Edge locations

Categories of AWS services

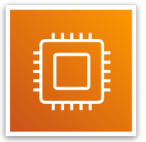

Analytics


Application Integration


AR and VR


Blockchain


Business Applications


Compute


Cost Management


Customer Engagement


Database


Developer Tools


End User Computing


Game Tech


Internet of Things


Machine Learning


Management and Governance


Media Services


Migration and Transfer


Mobile


Networking and Content Delivery


Robotics


Satellite


Security, Identity, and Compliance


Storage

Storage service category

Photo from https://www.pexels.com/photo/black-and-grey-device-159282/

AWS storage services

Amazon Simple Storage Service (Amazon S3)

Amazon Elastic Block Store (Amazon EBS)

Amazon Elastic File System (Amazon EFS)

Amazon Simple Storage Service Glacier

Compute service category

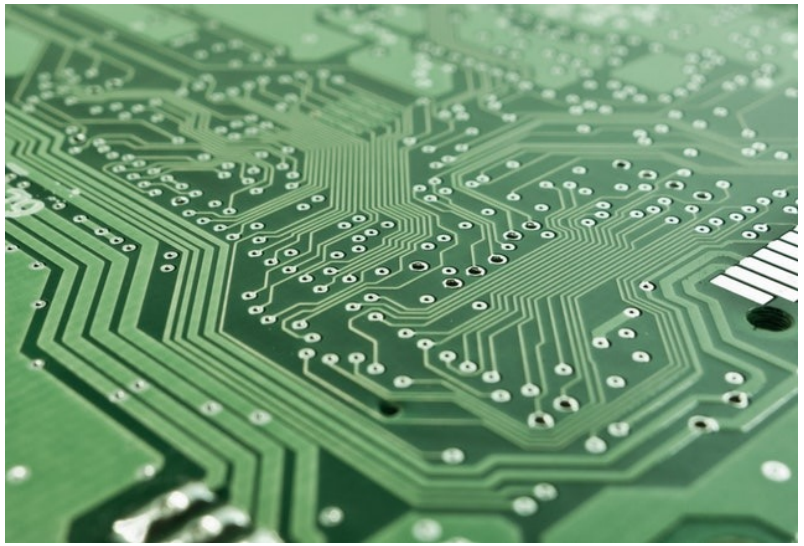


Photo from https://www.pexels.com/photo/technology-computer-lines-board-50711/

AWS Compute services

- Amazon EC2
- Amazon EC2 Auto Scaling
- Amazon Elastic Container Service (Amazon ECS)
- Amazon EC2 Container Registry
- AWS Elastic Beanstalk
- AWS Lambda
- Amazon Elastic Kubernetes Service (Amazon EKS)
- AWS Fargate

Database service category

Photo from https://aws.amazon.com/compliance/data-center/data-centers/

AWS Database services

- Amazon Relational Database Service
- Amazon Aurora
- Amazon Redshift
- Amazon DynamoDB

Networking and content delivery service category

Photo by Umberto on Unsplash

AWS networking and content delivery services

- Amazon VPC
- Elastic Load Balancing
- Amazon CloudFront
- AWS Transit Gateway
- Amazon Route 53
- AWS Direct Connect
- AWS VPN

Security, identity, and compliance service category

Photo by Paweł Czerwiński on Unsplash

AWS security, identity, and compliance services

- AWS Identity and Access Management (IAM)
- AWS Organizations
- Amazon Cognito
- AWS Artifact
- AWS Key Management Service
- AWS Shield

AWS cost management service category

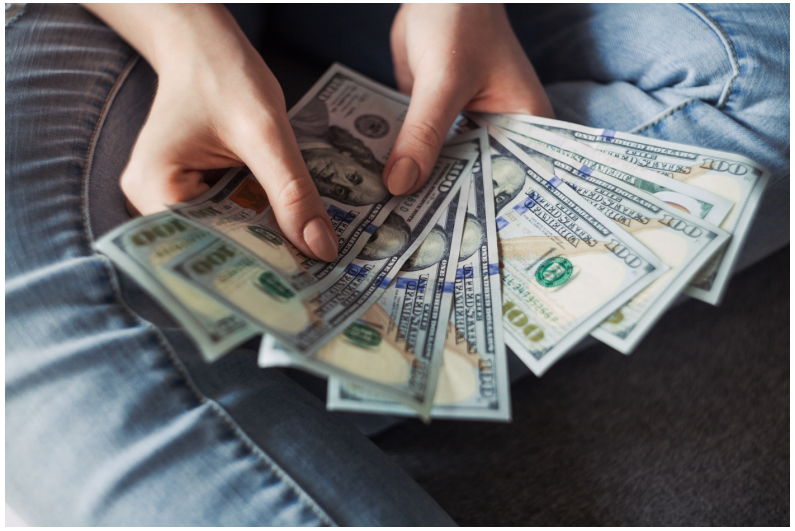


Photo by Alexander Mils on Unsplash

AWS cost management services

- AWS Cost and Usage Report
- AWS Budgets
- AWS Cost Explorer

Management and governance service category

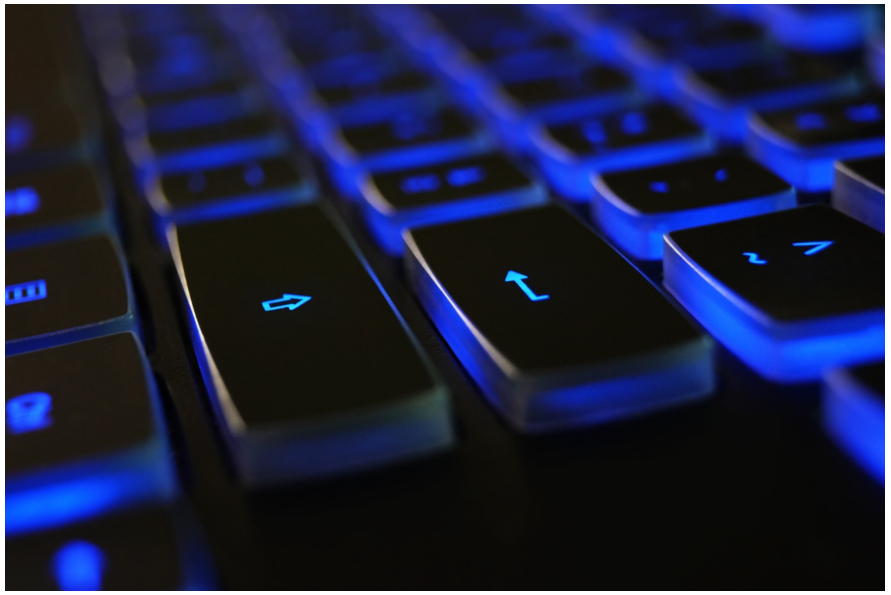
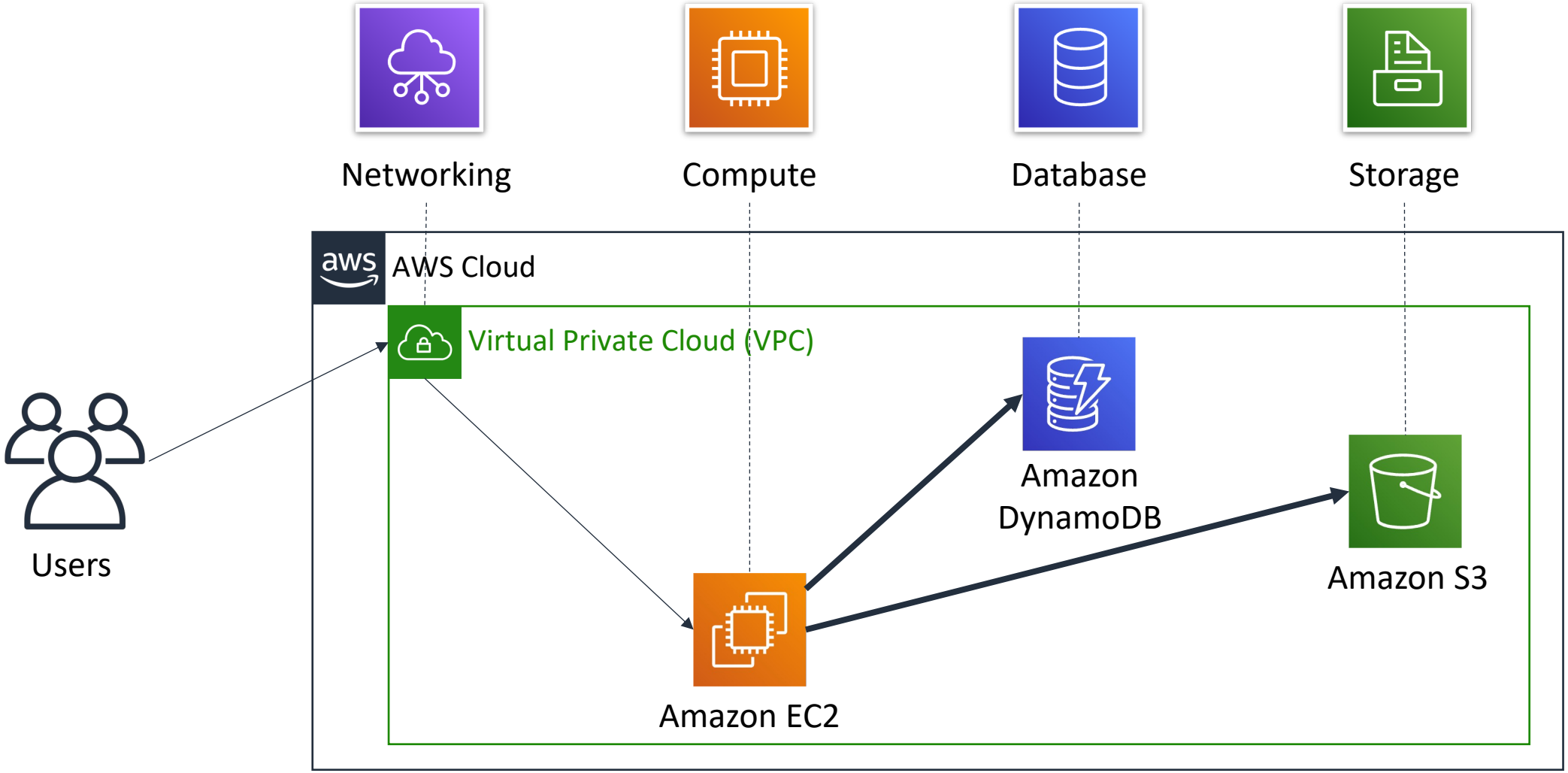


Photo by Marta Branco from Pexels

AWS management and governance services

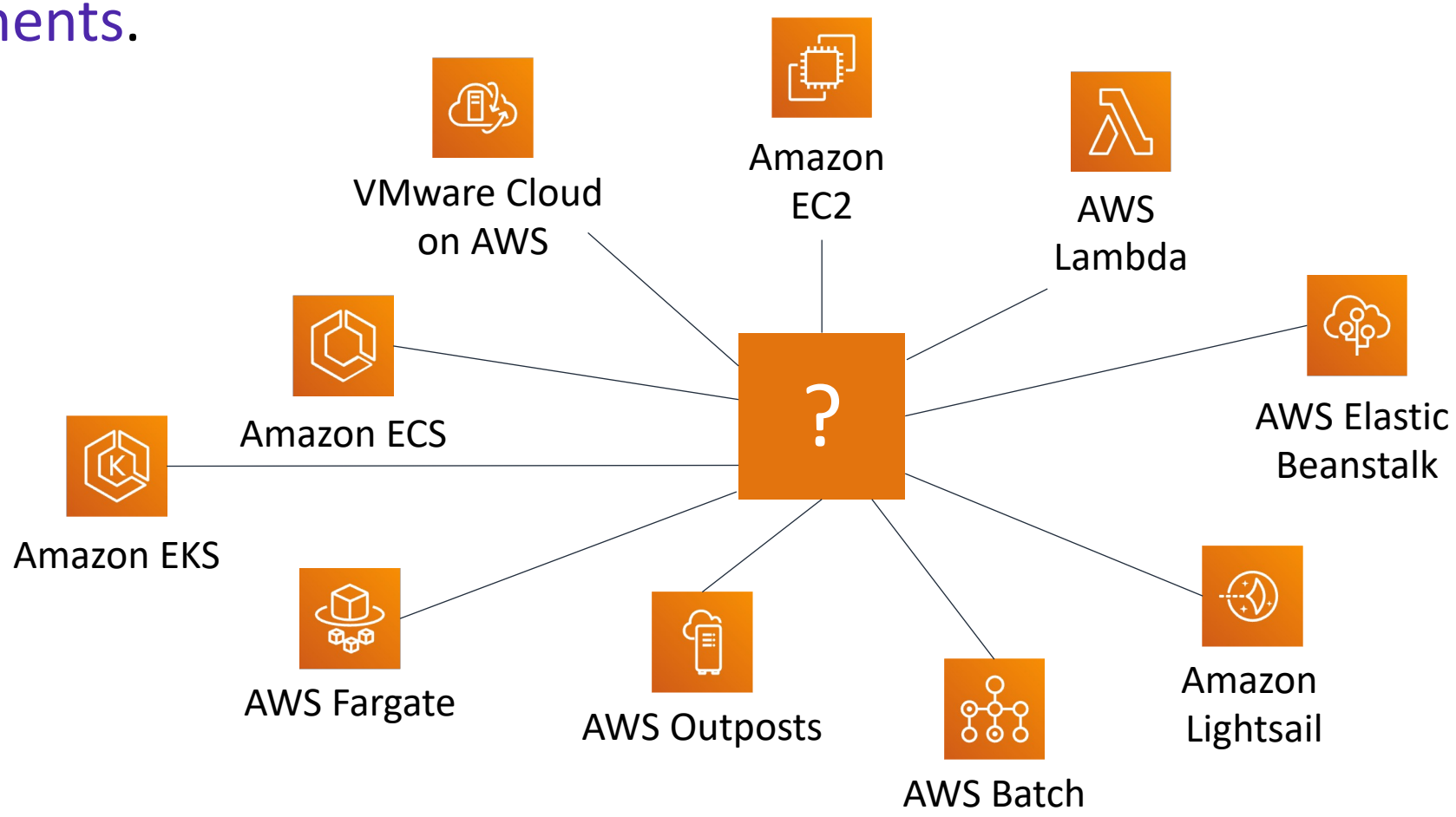
- AWS Management Console
- AWS Config
- Amazon CloudWatch
- AWS Auto Scaling
- AWS Command Line Interface
- AWS Trusted Advisor
- AWS Well-Architected Tool
- AWS CloudTrail

Simple solution example



Choosing a service

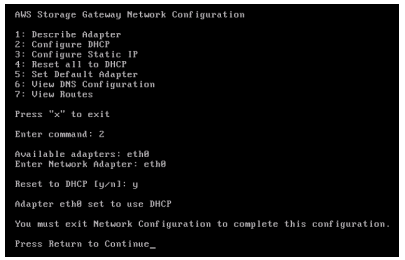
The service you select depends on your business goals and technology requirements.



Three ways to interact with AWS

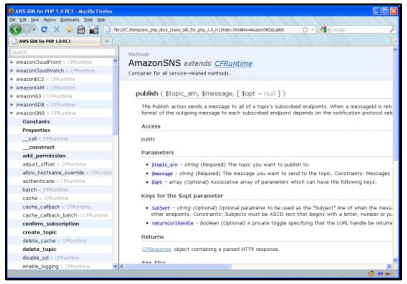
AWS Management Console

Easy-to-use graphical interface



Command Line Interface (AWS CLI)

Access to services by discrete commands or scripts



Software Development Kits (SDKs)

Access services directly from your code (such as Java, Python, and others)

Introduction to AWS

Fundamentals of Pricing and Technical Supports

AWS pricing model

Three fundamental drivers of cost with AWS

Compute

- Charged per hour/second*
- Varies by instance type

*Linux only

Storage

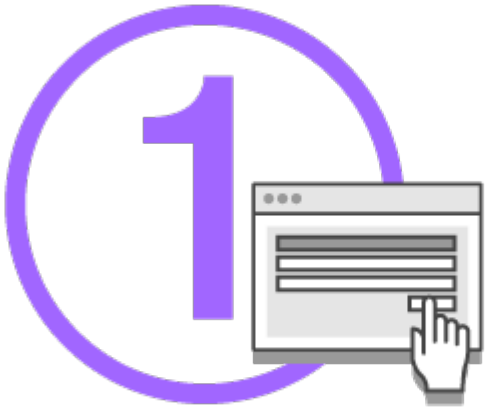
- Charged typically per GB

Data transfer

- Outbound is aggregated and charged
- Inbound has no charge (with some exceptions)
- Charged typically per GB

AWS Free Tier

Enables you to gain free hands-on experience with the AWS platform, products, and services. Free for 1 year for new customers.



Sign up for an AWS account

Learn with 10-minute tutorials

Start building with AWS

Services with no charge


Amazon VPC


Elastic Beanstalk**


Auto Scaling**

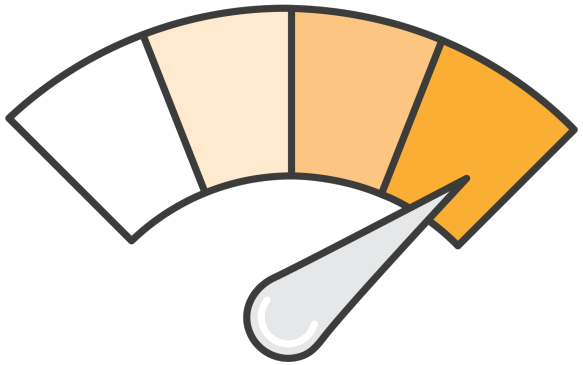

AWS CloudFormation**


AWS Identity and Access Management (IAM)

**Note: There might be charges associated with other AWS services that are used with these services.

Support plans

AWS Support offers four support plans:



- **Basic Support** – Resource Center access, Service Health Dashboard, product FAQs, discussion forums, and support for health checks
- **Developer Support**: Support for early development on AWS
- **Business Support**: Customers that run production workloads
- **Enterprise Support**: Customers that run business and mission-critical workloads

Case severity and response times

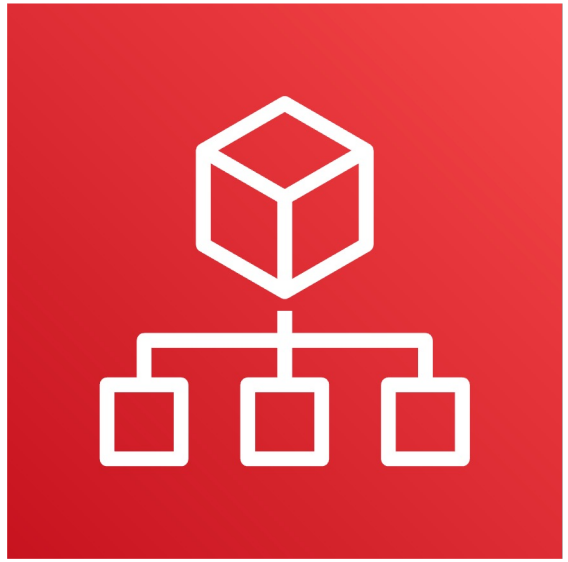
	Critical	Urgent	High	Normal	Low
Basic			No Case Support		
Developer Plan (Business hours)				12 hours or less	24 hours or less
Business Plan (24/7)		1 hour or less	4 hours or less	12 hours or less	24 hours or less
Enterprise Plan (24/7)	15 minutes or less	1 hour or less	4 hours or less	12 hours or less	24 hours or less

Introduction to AWS

AWS Organizations

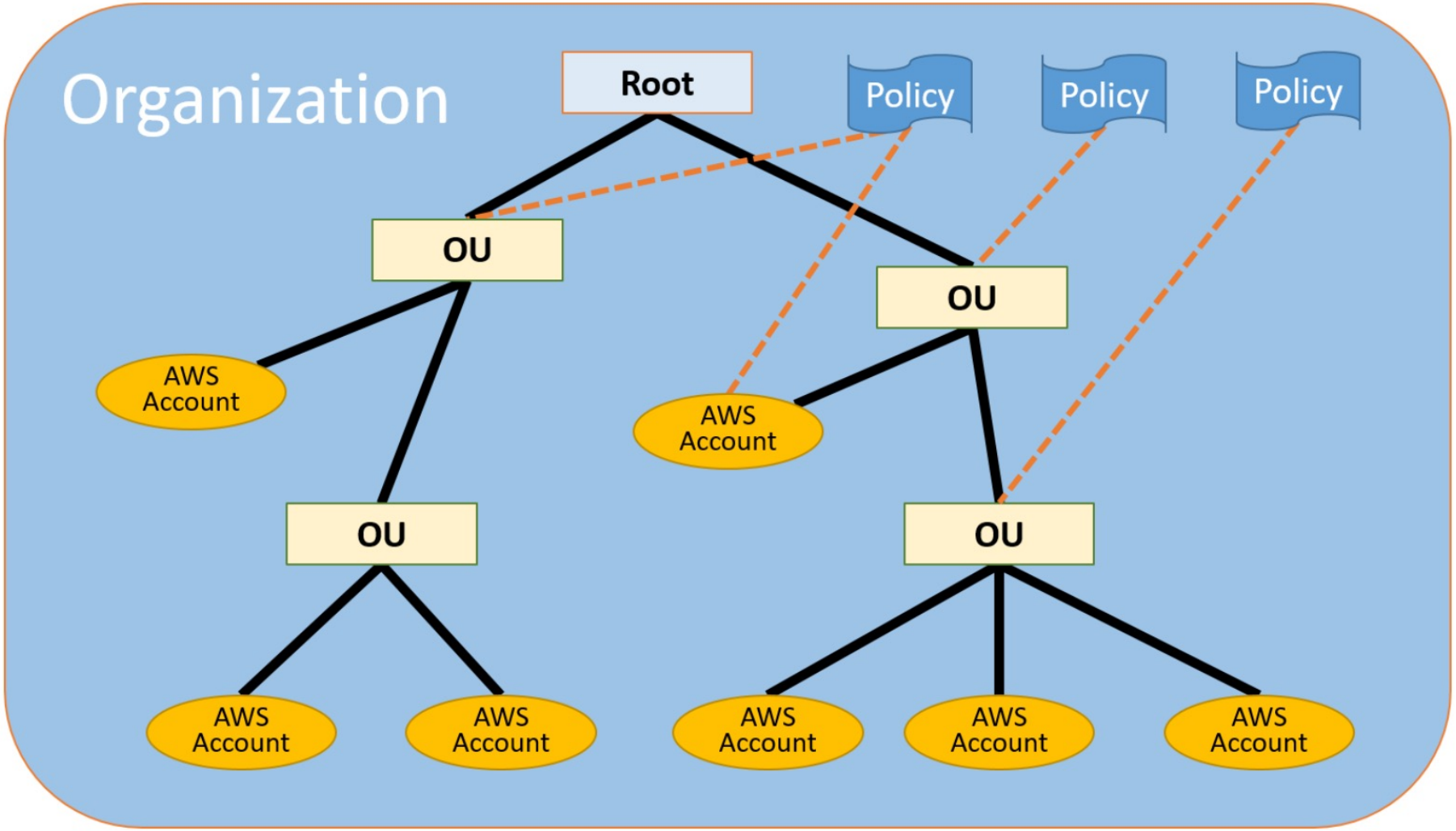
aws academy

Introduction to AWS Organizations



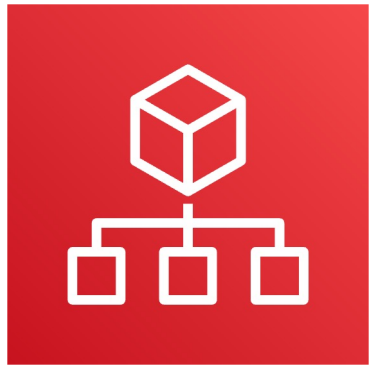
AWS Organizations

AWS Organizations terminology



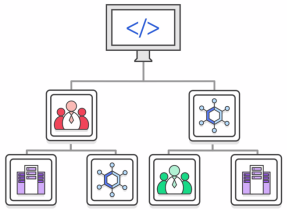
*Organizational Units (OUs)

Key features and benefits

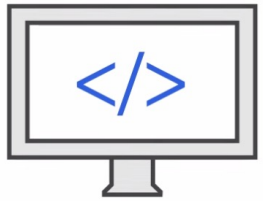


AWS Organizations

Policy-based account management



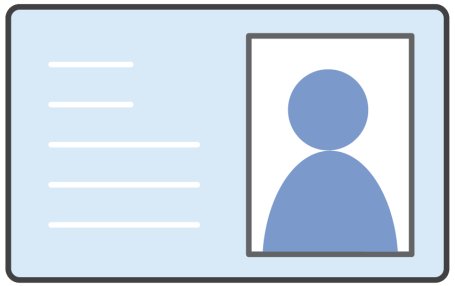
Group based account management



Application programming interfaces (APIs) that automate account management

Consolidated billing

Security with AWS Organizations

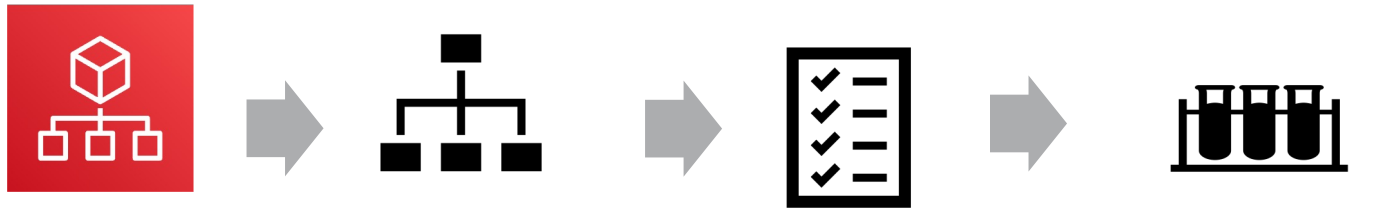


Control access with AWS Identity and Access Management (IAM).

IAM policies enable you to allow or deny access to AWS services for users, groups, and roles.

Service control policies (SCPs) enable you to allow or deny access to AWS services for individuals or group accounts in an organizational unit (OU).

Organizations setup



Step 1

Create Organization

Step 2

Create organizational units

Step 3

Create service control policies

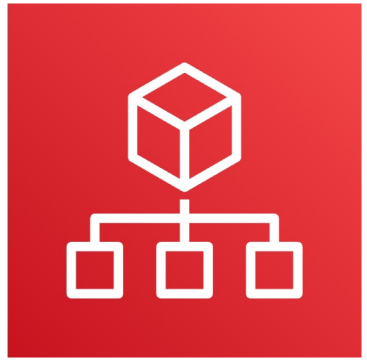
Step 4

Test restrictions

Limits of AWS Organizations

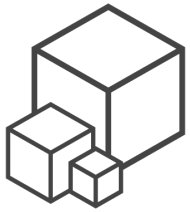
Limits		
Limits on Names	Names must be composed of Unicode characters.	
	Names must not exceed 250 characters in length.	
Maximum and Minimum Values	Number of AWS accounts	Varies. Note: An invitation sent to an account counts against this limit.
	Number of roots	1
	Number of OUs	1,000
	Number of policies	1,000
	Maximum size of a service control policy document	5,120 bytes
	Maximum nesting of OUs in a root	5 levels of OUs under a root
	Invitations sent per day	20
	Number of member accounts you can create concurrently	Only five can be in progress at one time
	Number of entities to which you can attach a policy	Unlimited

Accessing AWS Organizations



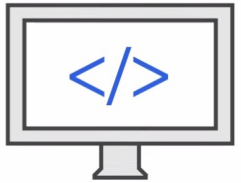
AWS Organizations

AWS Management Console



AWS Command Line Interface (AWS CLI) tools

Software development kits (SDKs)



HTTPS Query application programming interfaces (API)

Introduction to AWS

AWS Global Infrastructure

aws academy

AWS Global Infrastructure

- The **AWS Global Infrastructure** is designed and built to deliver a **flexible**, **reliable**, **scalable**, and **secure** cloud computing environment with high-quality **global network performance**.
- AWS continually updates its global infrastructure footprint. Visit one of the following web pages for current infrastructure information:
  - AWS Global Infrastructure Map
    Choose a circle on the map to view summary information about the Region represented by the circle.
  - Regions and Availability Zones
    Choose a tab to view a map of the selected geography and a list of Regions, Edge locations, Local zones, and Regional Caches.

AWS Regions

- An **AWS Region** is a geographical area.
  - Data replication across Regions is controlled by you.
  - Communication between Regions uses AWS backbone network infrastructure.
- Each Region provides full redundancy and connectivity to the network.
- A Region typically consists of two or more **Availability Zones**.

Example: London Region

Selecting a Region

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

Data governance, legal requirements

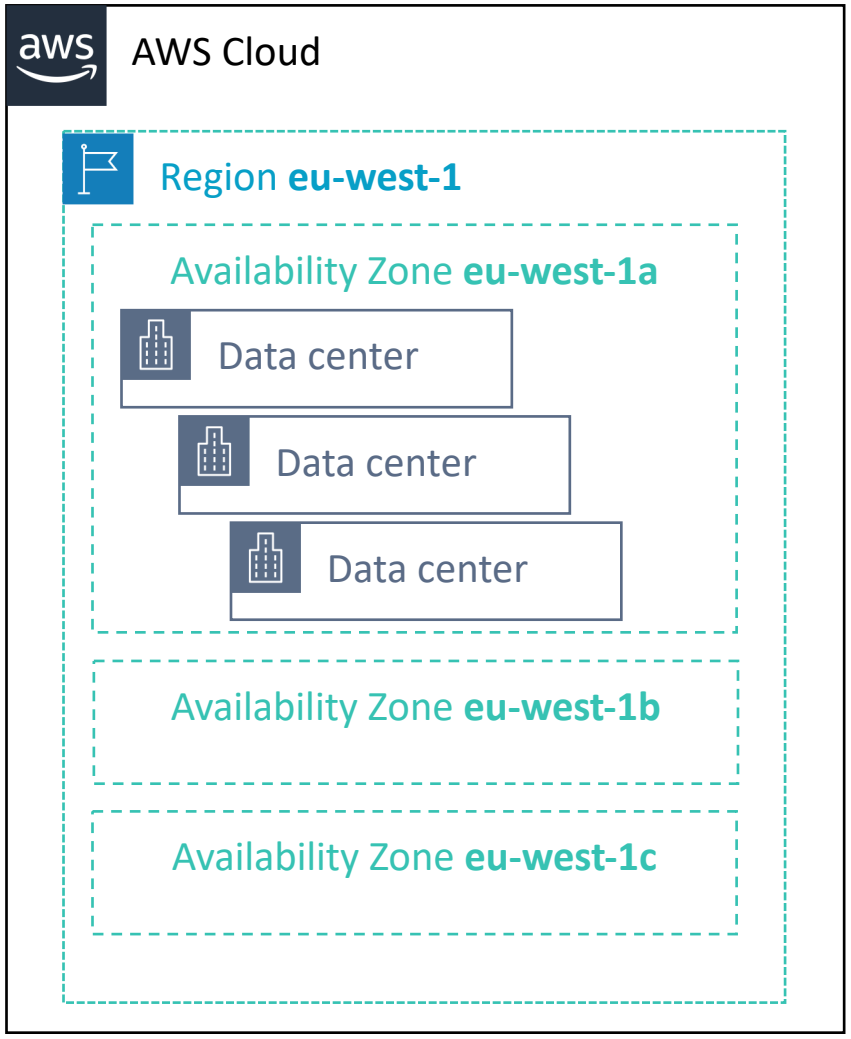
Proximity to customers (latency)

Services available within the Region

Costs (vary by Region)

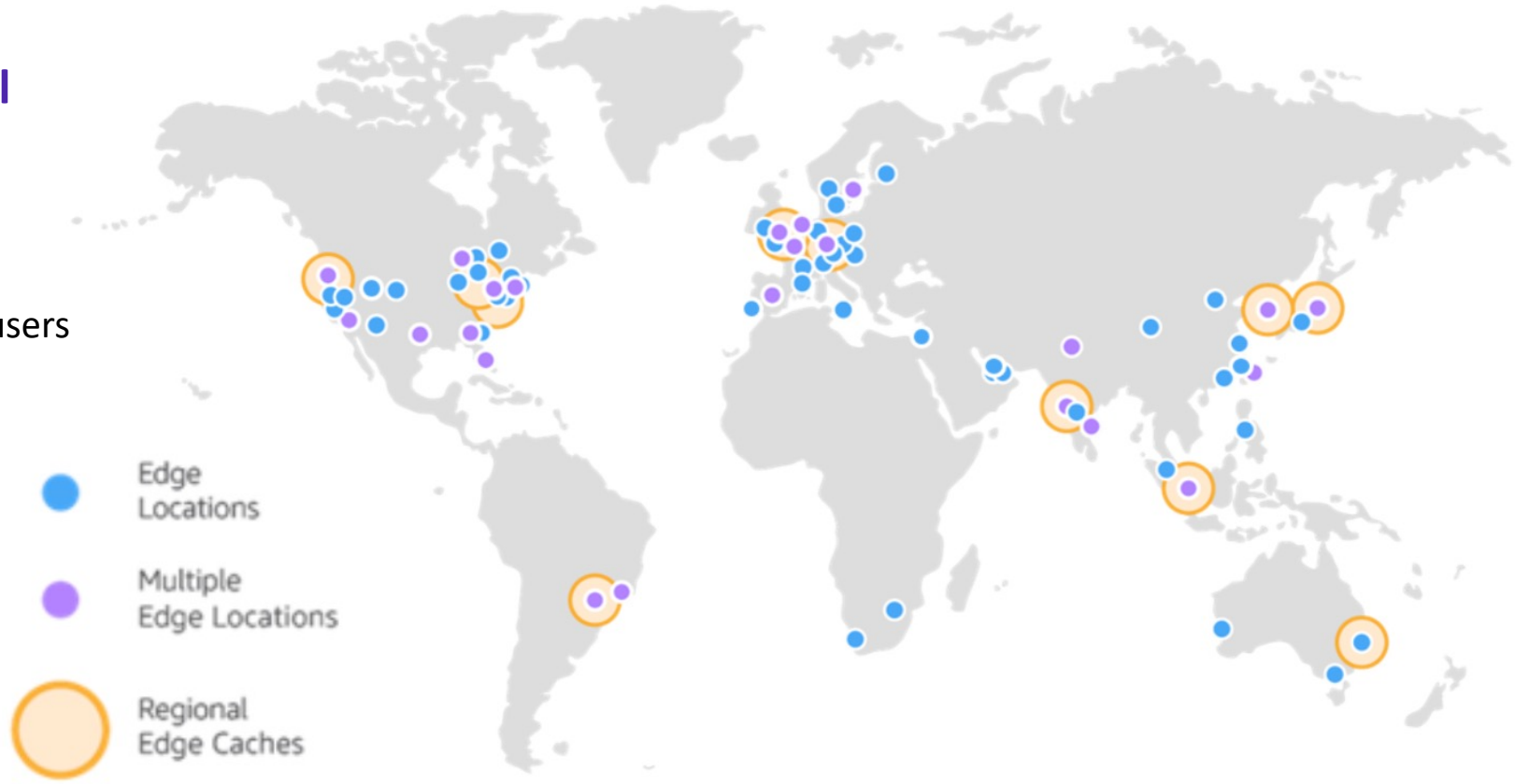
Availability Zones

- Each **Region** has multiple Availability Zones.
- Each **Availability Zone** is a fully isolated partition of the AWS infrastructure.
  - Availability Zones consist of discrete **data centers**
  - They are designed for fault isolation
  - They are interconnected with other Availability Zones by using high-speed private networking
  - You choose your Availability Zones.
  - **AWS recommends replicating data and resources across Availability Zones** for resiliency.



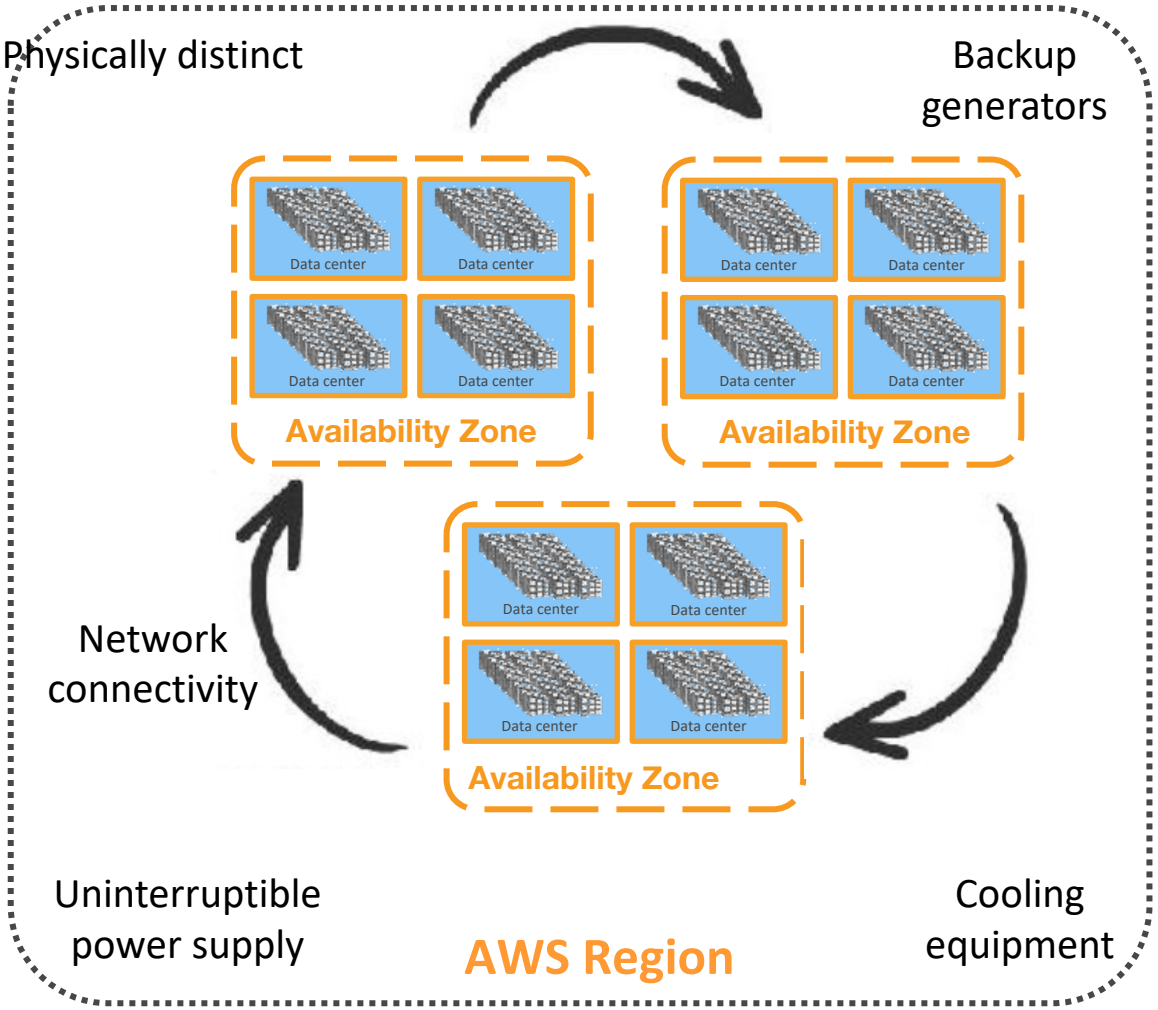
Points of Presence

- AWS provides a global network of Points of Presence locations
- Consists of **edge locations** and a much smaller number of **Regional edge caches**
- Used with Amazon CloudFront
  - A global Content Delivery Network (CDN), that delivers content to end users with reduced latency
- Regional edge caches used for content with infrequent access.



AWS infrastructure features

- Elasticity and scalability
  - Elastic infrastructure; dynamic adaption of capacity
  - Scalable infrastructure; adapts to accommodate growth
- Fault-tolerance
  - Continues operating properly in the presence of a failure
  - Built-in redundancy of components
- High availability
  - High level of operational performance
  - Minimized downtime
  - No human intervention

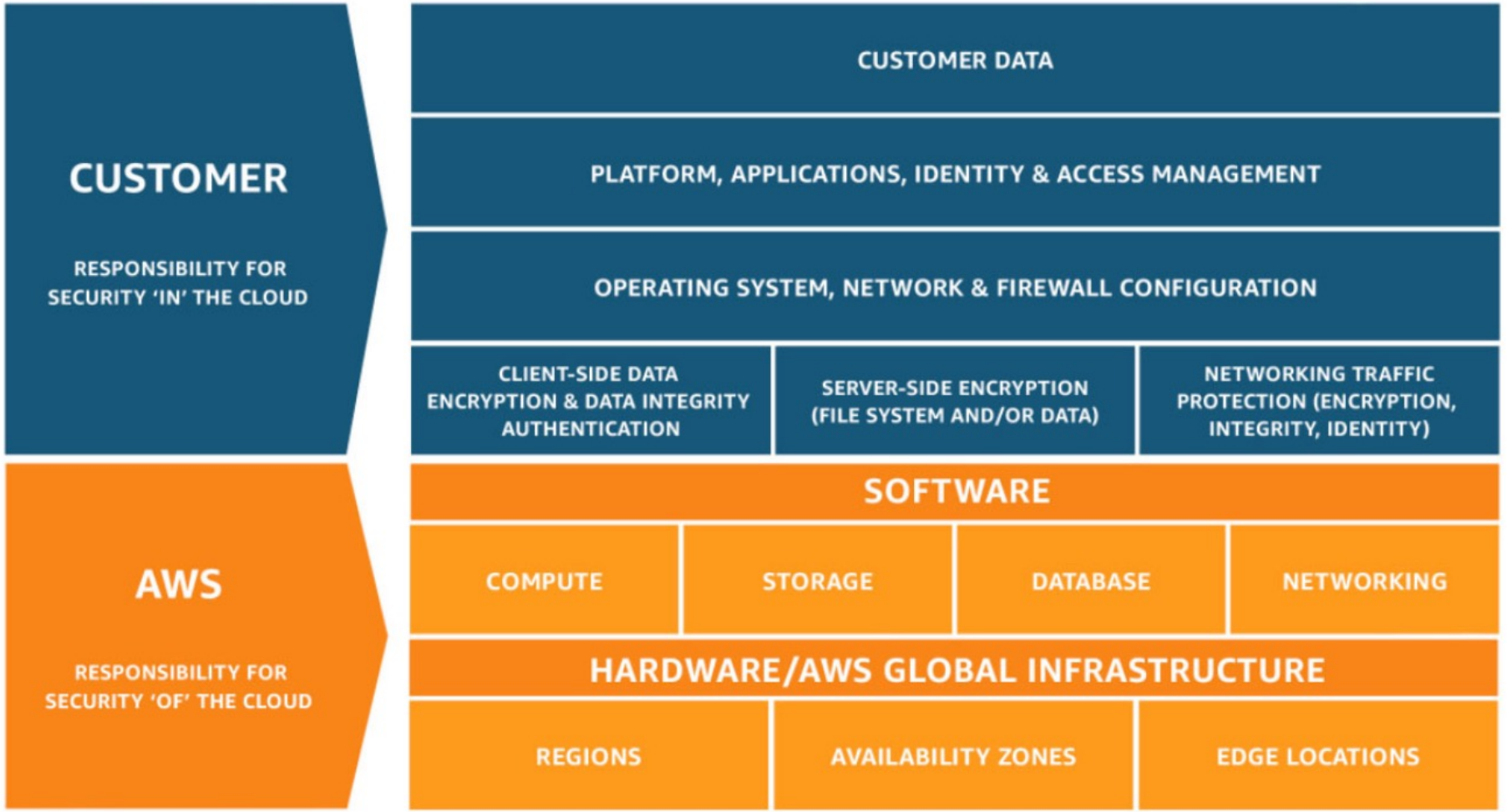


Introduction to AWS cloud security

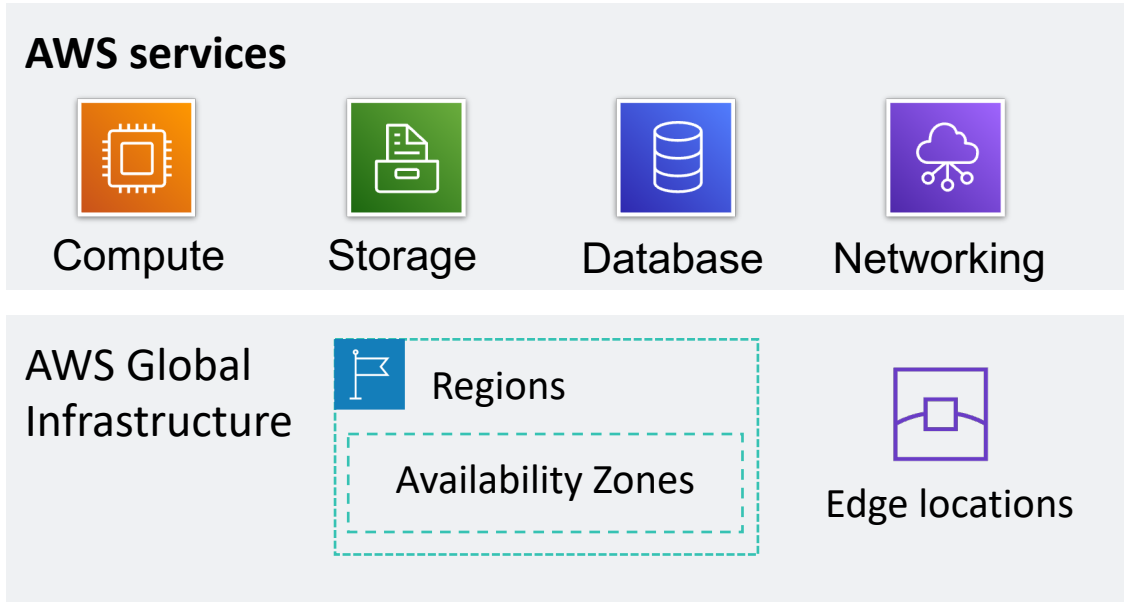
AWS Shared Responsibility Model

aws academy

AWS shared responsibility model



AWS responsibility: Security *of* the cloud

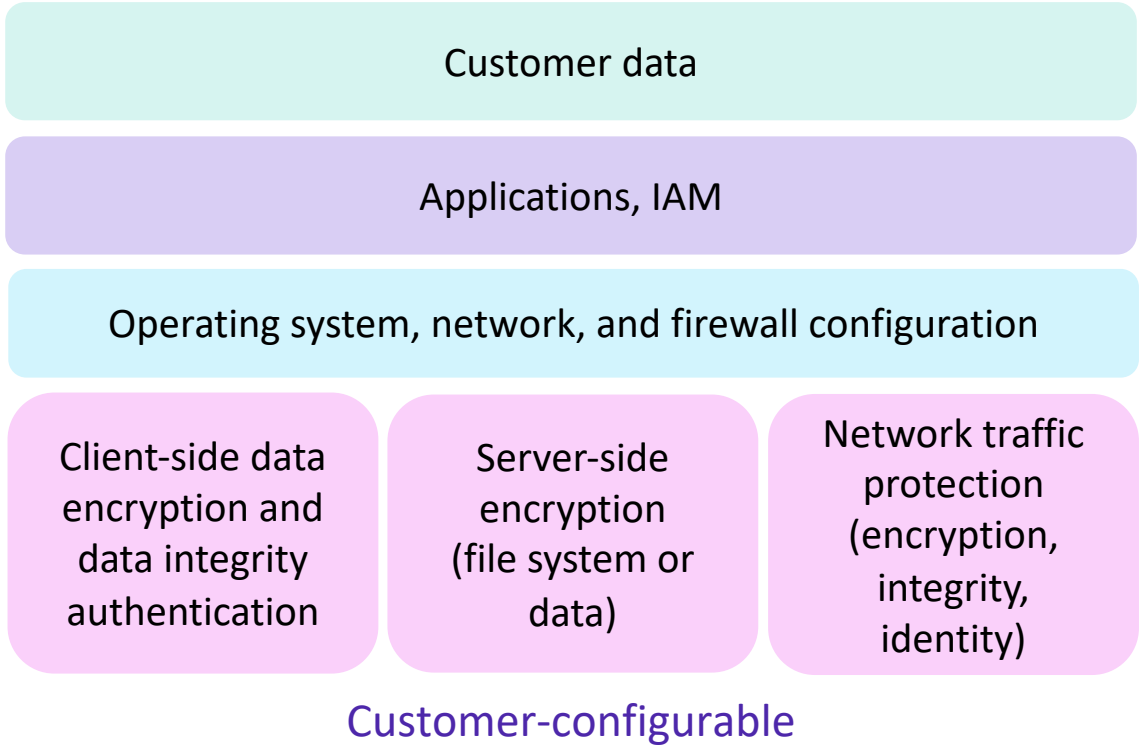


AWS responsibilities:

- Physical security of data centers
  - Controlled, need-based access
- Hardware and software infrastructure
  - Storage decommissioning, host operating system (OS) access logging, and auditing

- Network infrastructure
  - Intrusion detection
- Virtualization infrastructure
  - Instance isolation

Customer responsibility: Security *in* the cloud



Customer responsibilities:

- Amazon Elastic Compute Cloud (Amazon EC2) instance operating system
  - Including patching, maintenance
- Applications
  - Passwords, role-based access, etc.
- Security group configuration
- OS or host-based firewalls
  - Including intrusion detection or prevention systems
- Network configurations
- Account management
  - Login and permission settings for each user

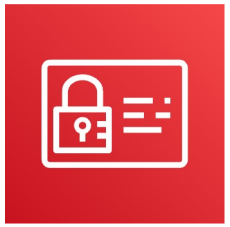
Introduction to AWS Cloud Security

AWS Identity and Access Management (IAM)

aws academy

AWS Identity and Access Management (IAM)

- Use **IAM** to manage access to **AWS resources** –
  - A resource is an entity in an AWS account that you can work with
  - Example resources; An Amazon EC2 instance or an Amazon S3 bucket
- *Example* – Control who can terminate Amazon EC2 instances
- Define fine-grained access rights –
  - **Who** can access the resource
  - **Which** resources can be accessed and what can the user do to the resource
  - **How** resources can be accessed
- IAM is a no-cost AWS account feature



AWS Identity and Access Management (IAM)

IAM: Essential components

IAM user

A **person** *or* **application** that can authenticate with an AWS account.

IAM group

A **collection of IAM users** that are granted identical authorization.

IAM policy

The document that defines **which resources can be accessed** and the **level of access** to each resource.

IAM role

Useful mechanism to grant a set of permissions for making AWS service requests.

Authenticate as an IAM user to gain access

When you define an **IAM user**, you select what ***types of access*** the user is permitted to use.

Programmatic access

- Authenticate using:
  - Access key ID
  - Secret access key
- Provides AWS CLI and AWS SDK access

AWS CLI

AWS Tools and SDKs

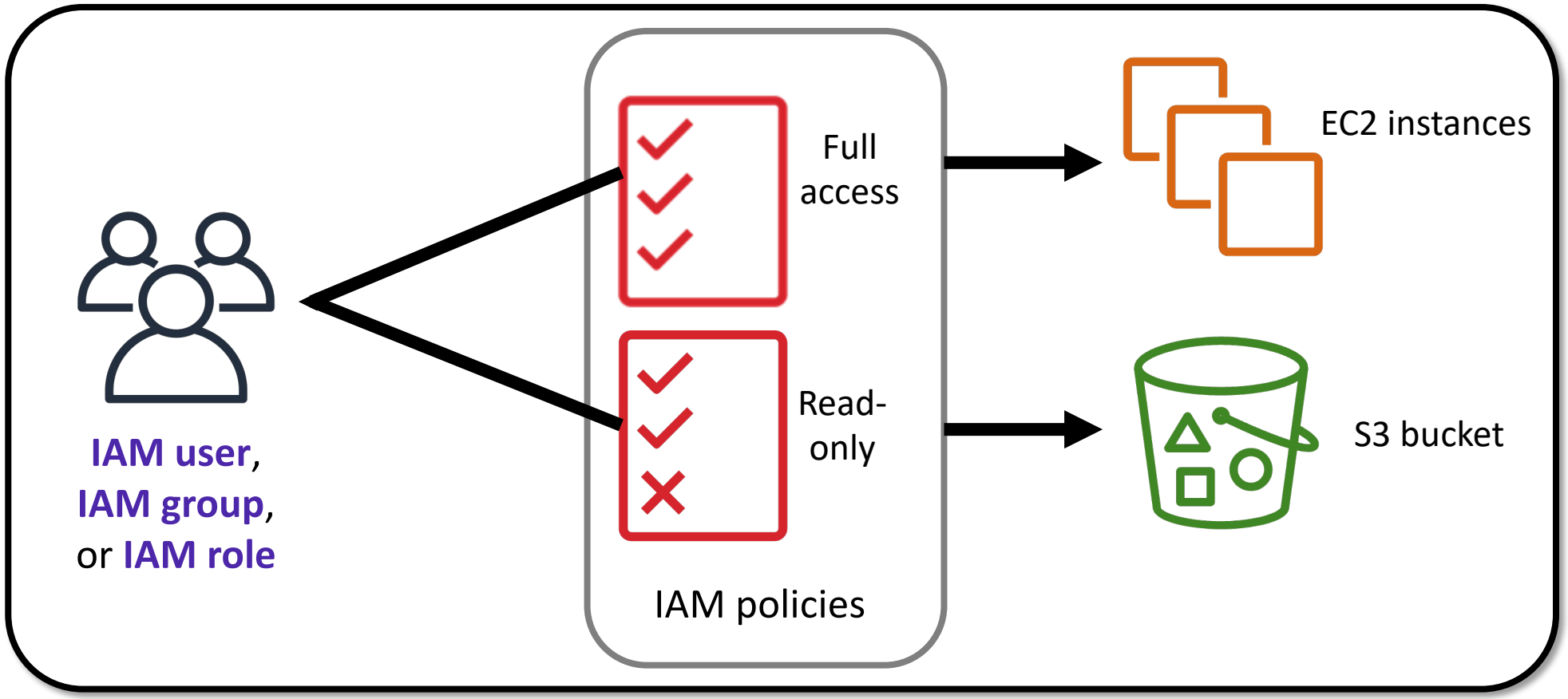
AWS Management Console access

- Authenticate using:
  - 12-digit Account ID *or* alias
  - IAM user name
  - IAM password
- If enabled, **multi-factor authentication (MFA)** prompts for an authentication code.

AWS Management Console

Authorization: What actions are permitted

After the user or application is connected to the AWS account, what are they allowed to do?



IAM: Authorization

- Assign permissions by creating an IAM policy.
- Permissions determine **which resources and operations** are allowed:
  - All permissions are implicitly denied by default.
  - If something is explicitly denied, it is never allowed.

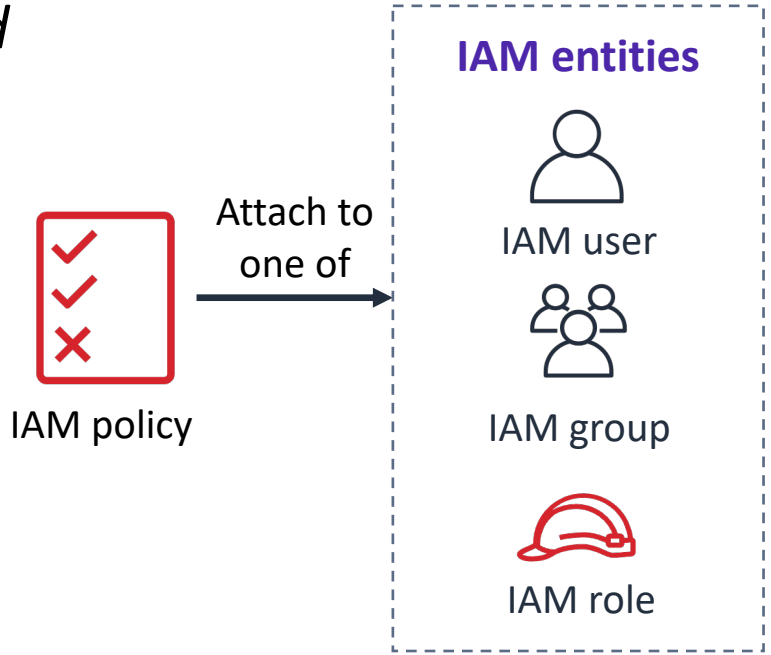
Best practice: Follow the **principle of least privilege**.

IAM permissions

Note: The scope of IAM service configurations is **global**. Settings apply across all AWS Regions.

IAM policies

- **An IAM policy is a document that defines permissions**
  - Enables fine-grained access control
- Two types of policies – *identity-based* and *resource-based*
- **Identity-based** policies –
  - Attach a policy to any IAM entity
    - An IAM user, an IAM group, or an IAM role
  - Policies specify:
    - Actions that ***may*** be performed by the entity
    - Actions that ***may not*** be performed by the entity
  - A single *policy* can be attached to multiple *entities*
  - A single *entity* can have multiple *policies* attached to it
- **Resource-based** policies
  - Attached to a resource (such as an S3 bucket)



IAM policy example

```
{
  "Version": "2012-10-17",
  "Statement":[{
    "Effect":"Allow",
    "Action":["DynamoDB:*","s3:*"],
    "Resource":[
      "arn:aws:dynamodb:region:account-number-without-hyphens:table/table-name",
      "arn:aws:s3:::bucket-name",
      "arn:aws:s3:::bucket-name/*"]
    },
    {
    "Effect":"Deny",
    "Action":["dynamodb:*","s3:*"],
    "NotResource":["arn:aws:dynamodb:region:account-number-without-hyphens:table/table-name”,
      "arn:aws:s3:::bucket-name",
      "arn:aws:s3:::bucket-name/*"]
    }
  ]
}
```

Explicit allow gives users access to a specific DynamoDB table and…

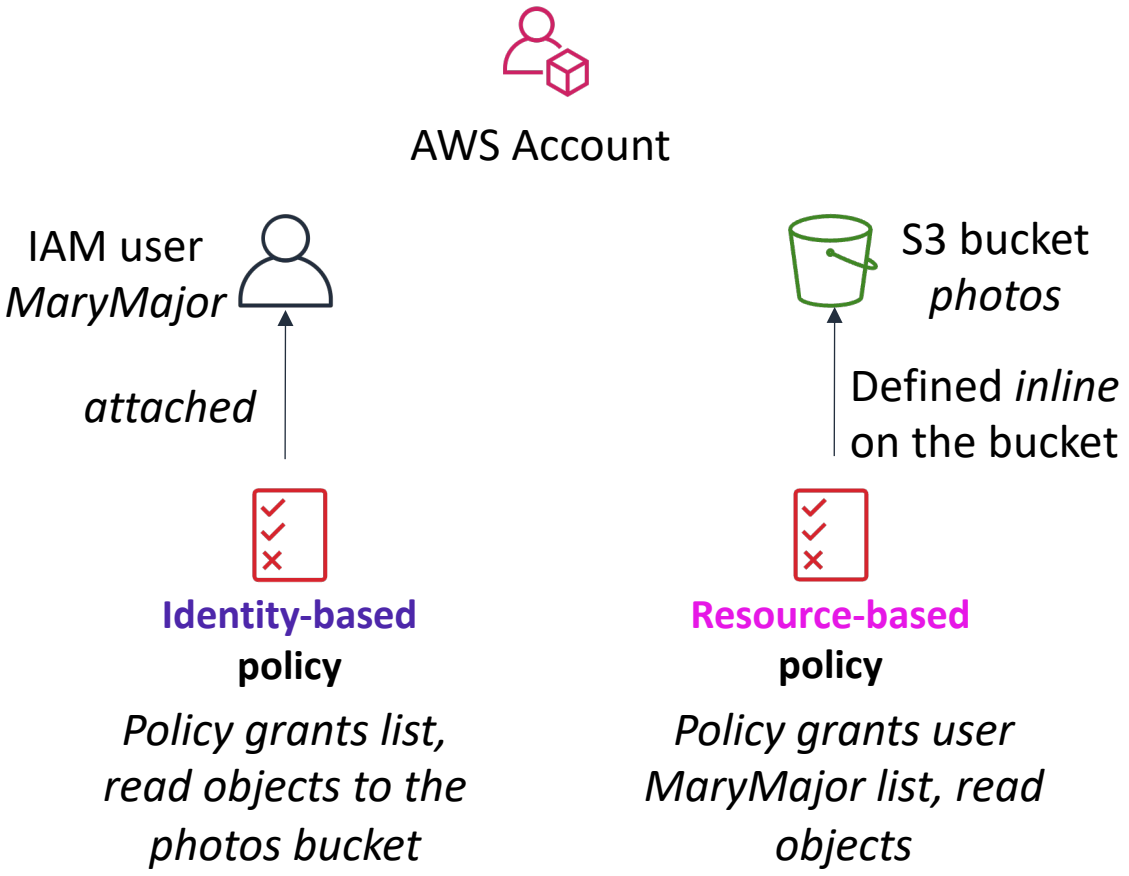
…Amazon S3 buckets.

Explicit deny ensures that the users cannot use any other AWS actions or resources other than that table and those buckets.

An explicit deny statement **takes precedence** over an allow statement.

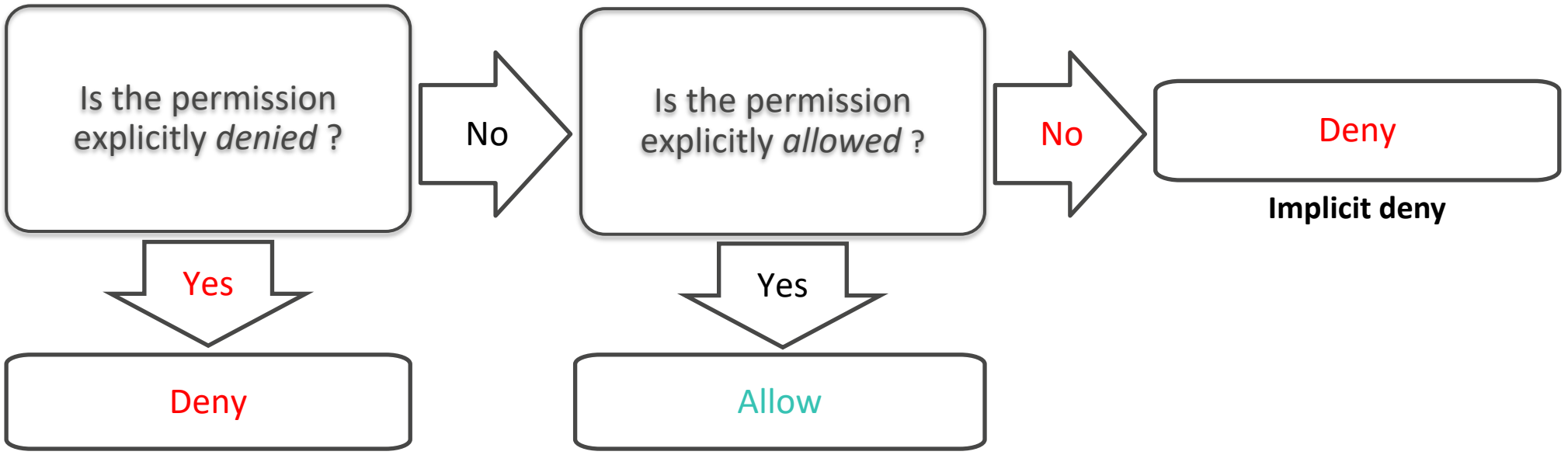
Resource-based policies

- *Identity-based policies* are attached to a user, group, or role
- **Resource-based policies** are attached to a resource (*not* to a user, group or role)
- Characteristics of resource-based policies –
  - Specifies who has access to the resource and what actions they can perform on it
  - The policies are *inline* only, not managed
- Resource-based policies are supported only by some AWS services



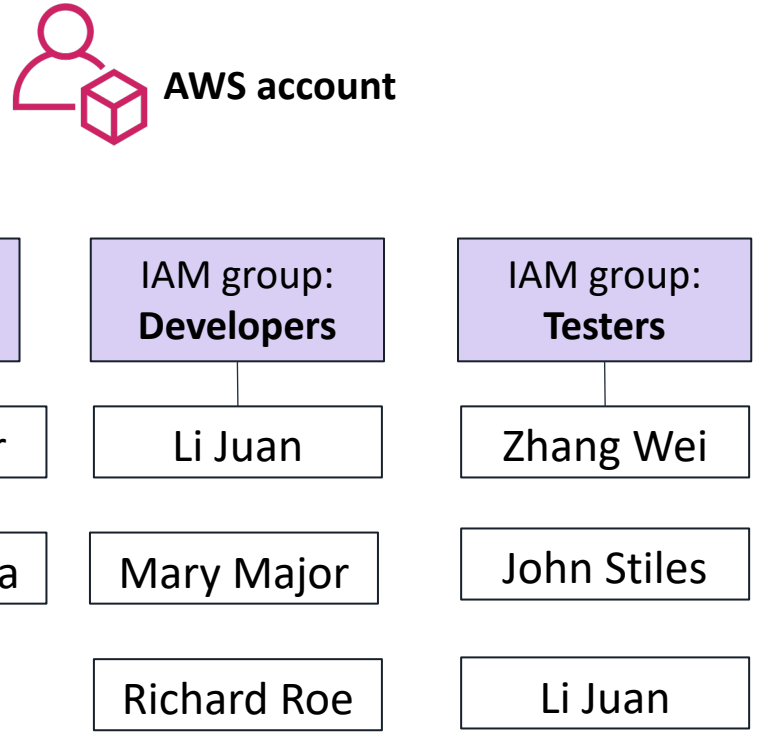
IAM permissions

How IAM determines permissions:



IAM groups

- An **IAM group** is a collection of IAM users
- A group is used to grant the same permissions to multiple users
  - Permissions granted by attaching IAM *policy* or policies to the group
- A user can belong to multiple groups
- There is no default group
- Groups cannot be nested



IAM roles

- An **IAM role** is an IAM identity with specific permissions
- Similar to an IAM user
  - Attach permissions policies to it
- Different from an IAM user
  - Not uniquely associated with one person
  - Intended to be *assumable* by a **person**, **application**, or **service**
- Role provides *temporary* security credentials
- Examples of how IAM roles are used to **delegate** access –
  - Used by an IAM user in the same AWS account as the role
  - Used by an AWS service—such as Amazon EC2—in the same account as the role
  - Used by an IAM user in a different AWS account than the role

IAM role

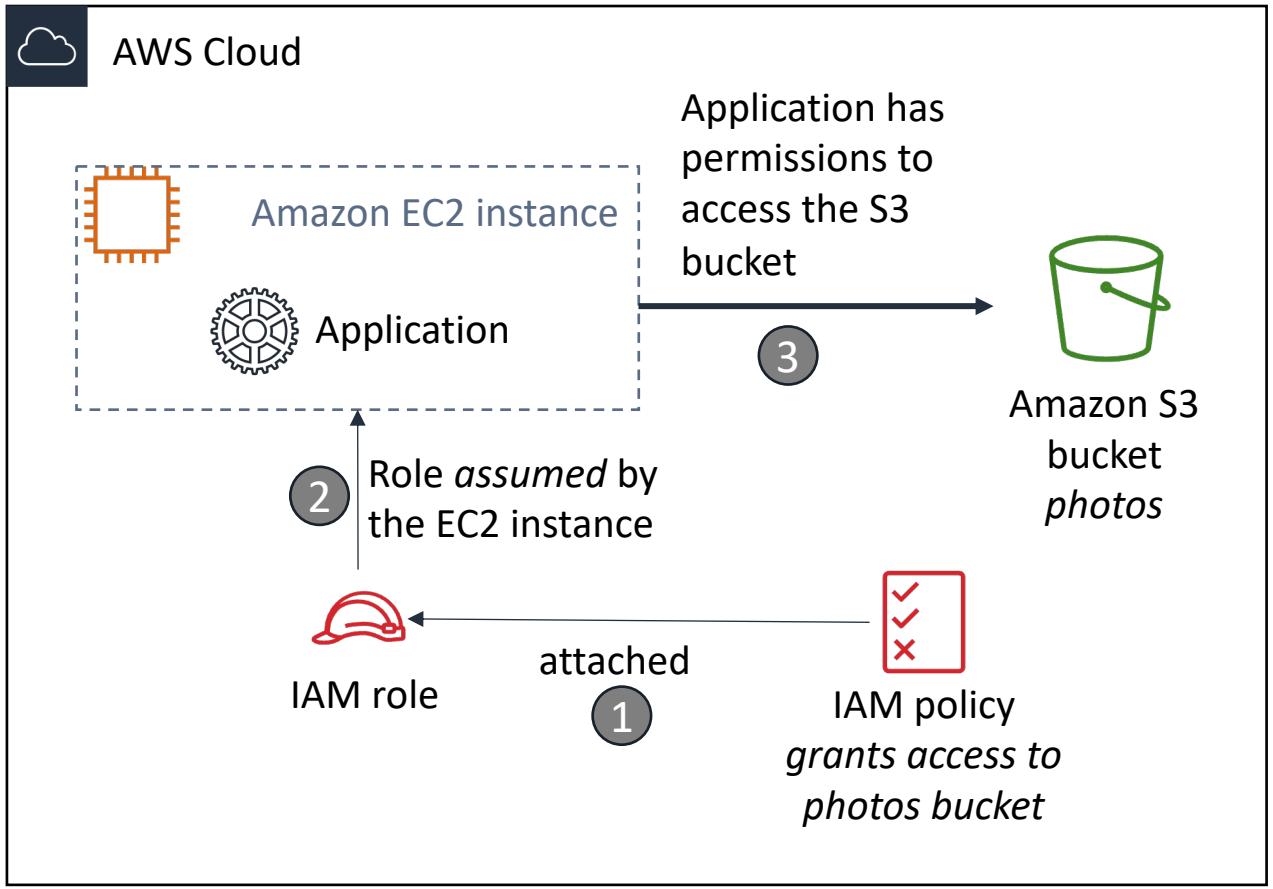
Example use of an IAM role

Scenario:

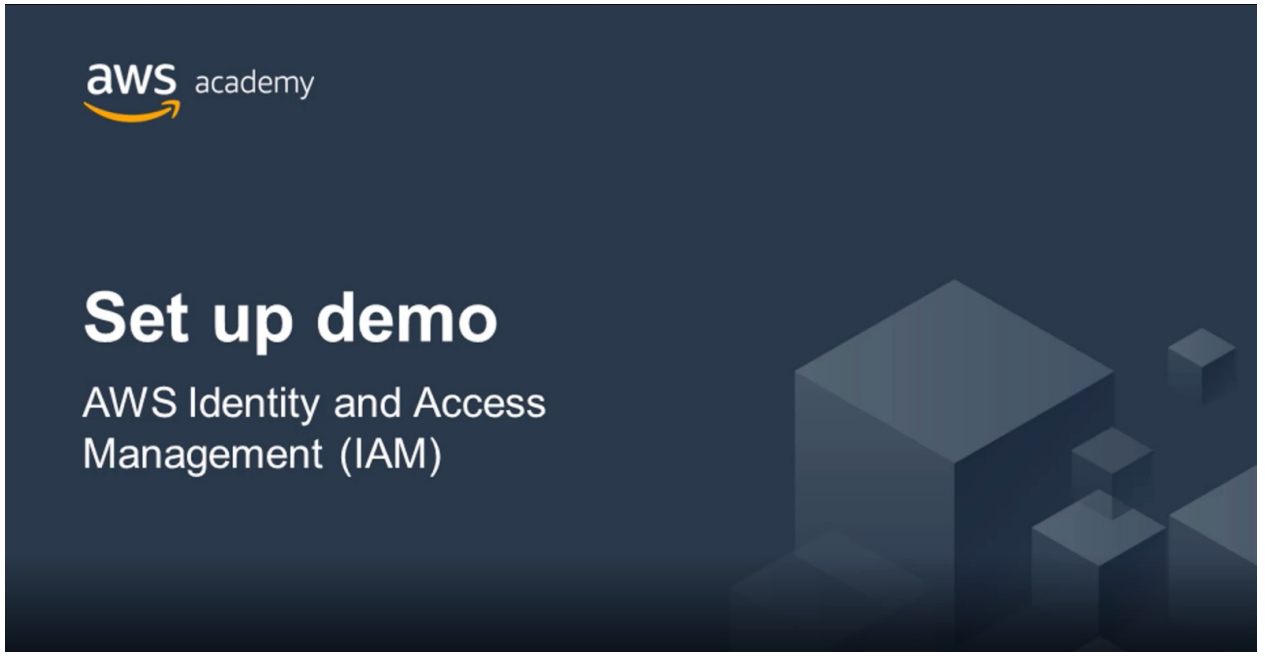
- An application that runs on an EC2 instance needs access to an S3 bucket

Solution:

- Define an IAM policy that grants access to the S3 bucket.
- Attach the policy to a role
- Allow the EC2 instance to assume the role



Recorded demo: IAM

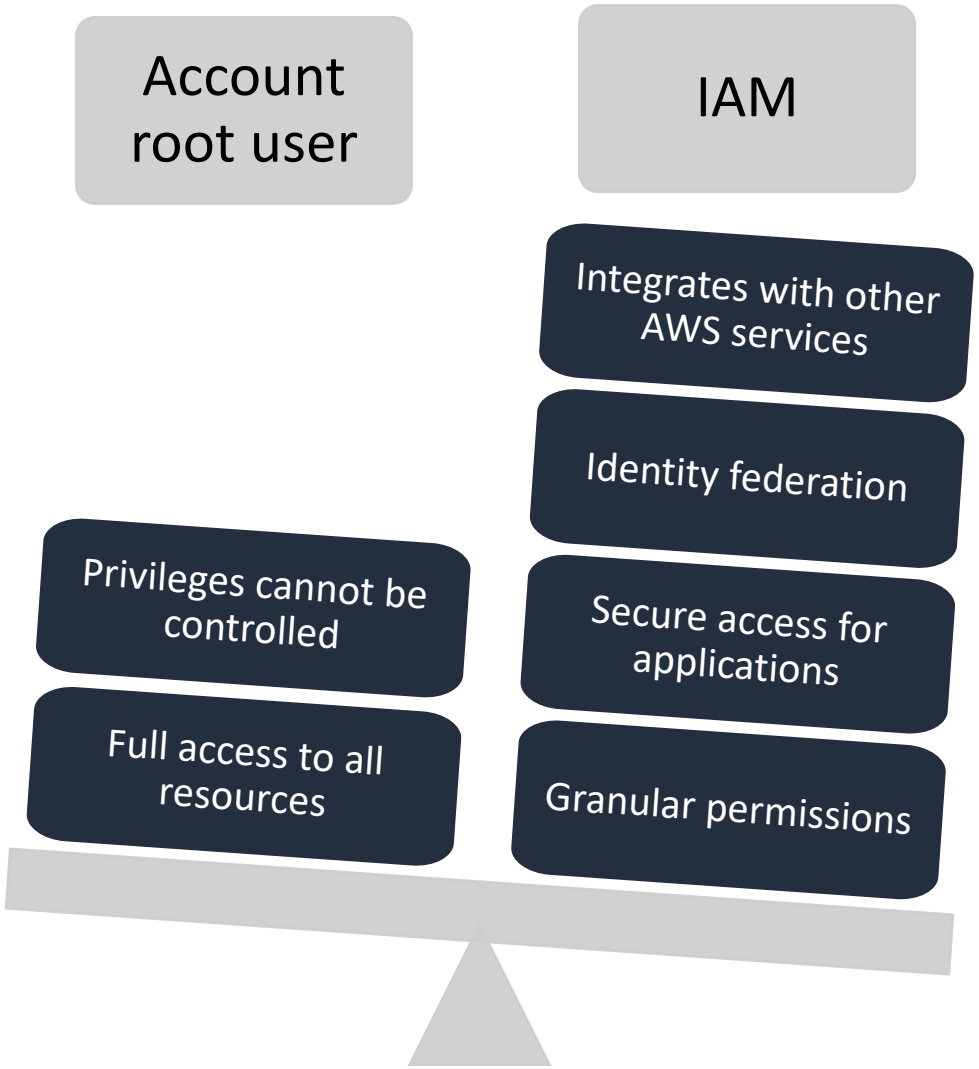


Introduction to AWS Cloud Security

Securing a New AWS Account

aws academy

AWS account root user access versus IAM access



- **Best practice**: Do not use the AWS account root user except when necessary.
  - Access to the **account root user** requires logging in with the *email address* (and password) that you used to create the account.
- Example actions that can only be done with the account root user:
  - Update the account root user password
  - Change the AWS Support plan
  - Restore an IAM user's permissions
  - Change account settings (for example, contact information, allowed Regions)

Securing a new AWS account: Account root user

Step 1: Stop using the account root user as soon as possible.

- The account root user has unrestricted access to all your resources.

- To stop using the account root user:
  1. While you are logged in as the account root user, create an IAM user for yourself. Save the access keys if needed.
  2. Create an IAM group, give it full administrator permissions, and add the IAM user to the group.
  3. Disable and remove your account root user access keys, if they exist.
  4. Enable a password policy for users.
  5. Sign in with your new IAM user credentials.
  6. Store your account root user credentials in a secure place.

Securing a new AWS account: MFA

Step 2: Enable multi-factor authentication (MFA).

- Require MFA for your account root user and for all IAM users.
- You can also use MFA to control access to AWS service APIs.

- Options for retrieving the MFA token –
  - Virtual MFA-compliant applications:
    - Google Authenticator.
    - Authy Authenticator (Windows phone app).
  - U2F security key devices:
    - For example, YubiKey.
  - Hardware MFA options:
    - Key fob or display card offered by Gemalto.

MFA token

Securing a new AWS account: AWS CloudTrail

Step 3: Use AWS CloudTrail.

- CloudTrail tracks user activity on your account.
  - Logs all API requests to resources in all supported services your account.
- Basic AWS CloudTrail event history is enabled by default and is free.
  - It contains all management event data on latest 90 days of account activity.

- To access CloudTrail –
  1. Log in to the **AWS Management Console** and choose the **CloudTrail** service.
  2. Click **Event history** to view, filter, and search the last 90 days of events.
- **To enable logs beyond 90 days and enable specified event alerting, create a trail.**
  1. From the CloudTrail Console trails page, click **Create trail**.
  2. Give it a name, apply it to all Regions, and create a new Amazon S3 bucket for log storage.
  3. Configure access restrictions on the S3 bucket (for example, only admin users should have access).

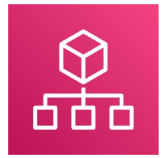
Introduction to AWS Cloud Security

Securing Accounts and Data on AWS

aws academy

AWS Organizations

- **AWS Organizations** enables you to consolidate multiple AWS accounts so that you centrally manage them.



AWS Organizations

- Security features of AWS Organizations:
  - **Group AWS accounts into organizational units** (OUs) and attach different access policies to each OU.
  - **Integration and support for IAM**
    - Permissions to a user are the intersection of what is allowed by AWS Organizations and what is granted by IAM in that account.
  - **Use service control policies** to establish control over the AWS services and API actions that each AWS account can access

AWS Organizations: Service control policies

- **Service control policies (SCPs)** offer centralized control over accounts.
  - Limit permissions that are available in an account that is part of an organization.
- Ensures that accounts comply with access control guidelines.
- 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.

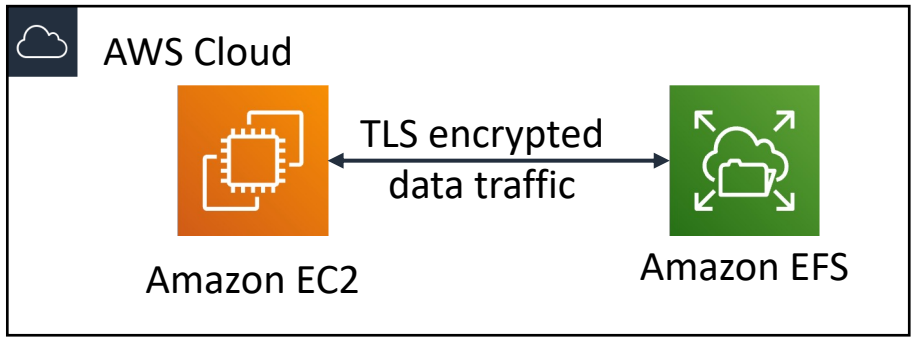
Encryption of data *at rest*

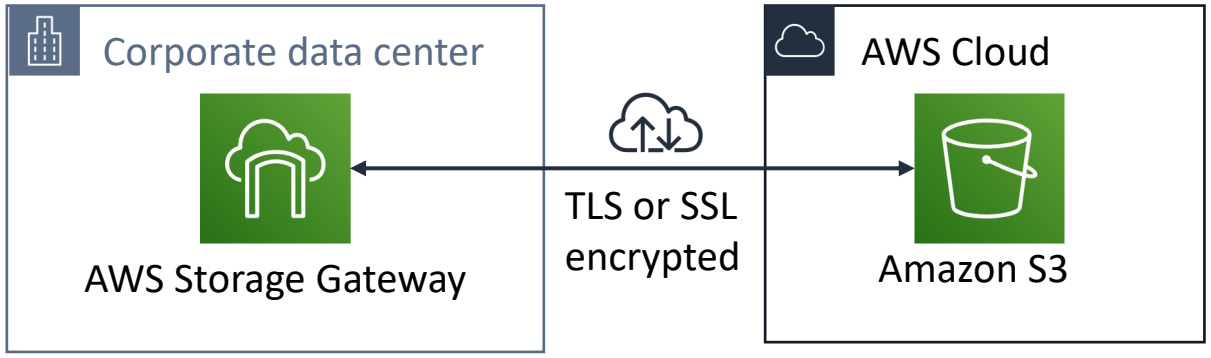
- **Encryption** encodes data with a secret key, which makes it unreadable
  - Only those who have the secret key can decode the data
  - AWS KMS can manage your secret keys

- AWS supports encryption of **data at rest**
  - Data at rest = Data stored physically (on disk or on tape)
  - You can encrypt data stored in any service that is supported by AWS KMS, including:
    - Amazon S3
    - Amazon EBS
    - Amazon Elastic File System (Amazon EFS)
    - Amazon RDS managed databases

Encryption of data *in transit*

- Encryption of **data in transit** (data moving across a network)
  - **Transport Layer Security (TLS)**—formerly SSL—is an open standard protocol
  - **AWS Certificate Manager** provides a way to manage, deploy, and renew TLS or SSL certificates
- Secure HTTP (HTTPS) creates a secure tunnel
  - Uses TLS or SSL for the bidirectional exchange of data
- **AWS services support data in transit encryption**.
  - Two examples:





Securing Amazon S3 buckets and objects

- Newly created S3 buckets and objects are private and protected by default.
- When use cases require sharing data objects on Amazon S3 –
  - It is essential to manage and control the data access.
  - Follow the **permissions that follow the principle of least privilege** and consider using Amazon S3 encryption.
- Tools and options for controlling access to S3 data include –
  - Amazon S3 Block Public Access feature: Simple to use.
  - IAM policies: A good option when the user can authenticate using IAM.
  - Bucket policies
  - Access control lists (ACLs): A legacy access control mechanism.
  - AWS Trusted Advisor bucket permission check: A free feature.

Lab 1: Introduction to IAM

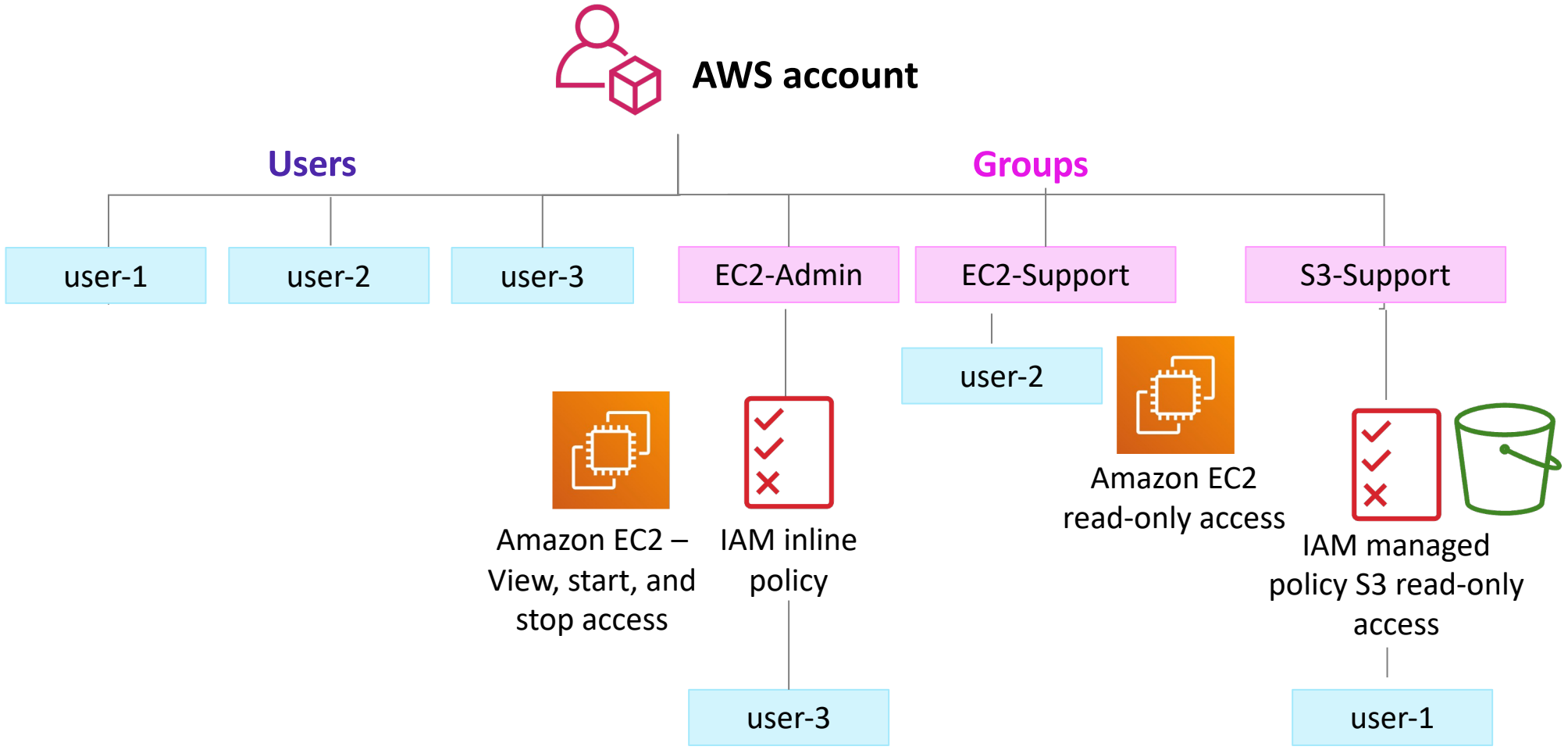
(~ 40 mins)

Lab 1: Tasks

- Task 1: Explore the Users and Groups.
- Task 2: Add Users to Groups.
- Task 3: Sign-In and Test Users.

AWS Identity and Access Management (IAM)

Lab 1: Final product



Q & A
Thank You

aws academy