Microsoft Azure

ABOUT TRAINER

My name is **Vishwanath Gowda H**, and I have over **13 years of experience in the IT industry**, working across domains such as **Cybersecurity, DevOps, and Multi-Cloud platforms including AWS, Azure, and GCP**. I am currently working as a **Platform Security Engineer**, where I focus on building secure, scalable, and automated solutions for enterprises. Along with my professional journey, I am passionate about **sharing knowledge with students** and guiding them to build strong careers in cloud computing and security.

WHAT IS CLOUD AND CLOUD COMPUTING

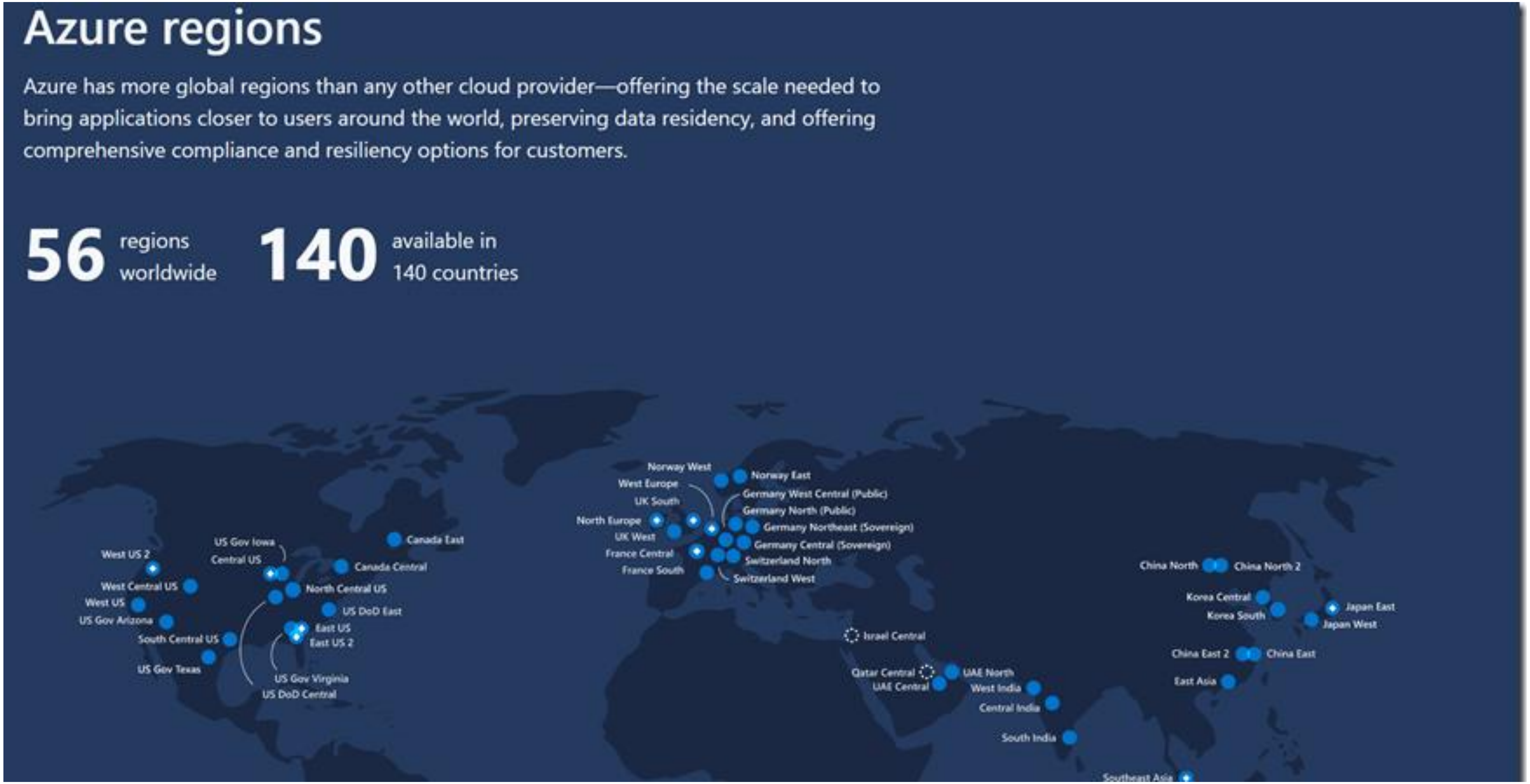
The **Cloud** refers to servers and resources (like storage, databases, networking, and software) that are delivered over the **internet**, instead of being managed on your local computer or data center.

Example: Instead of saving files on your laptop, you save them on **Google Drive or OneDrive** (that’s the cloud).

Cloud Computing is the delivery of IT services such as **servers, storage, databases, networking, software, and analytics** over the internet (“the cloud”) on a **pay-as-you-go basis**.

- You don’t need to buy and maintain expensive hardware.
- You can **access resources anytime, anywhere** through the internet.
- It provides **scalability, flexibility, cost savings, and reliability**.

Simple Example:
When you watch movies on **Netflix** or store photos in **Google Photos**, you’re already using cloud computing.



Azure regions

Azure has more global regions than any other cloud provider—offering the scale needed to bring applications closer to users around the world, preserving data residency, and offering comprehensive compliance and resiliency options for customers.

56 regions worldwide **140** available in 140 countries

TYPES OF CLOUD SERVICES

IaaS (Infrastructure as a Service)

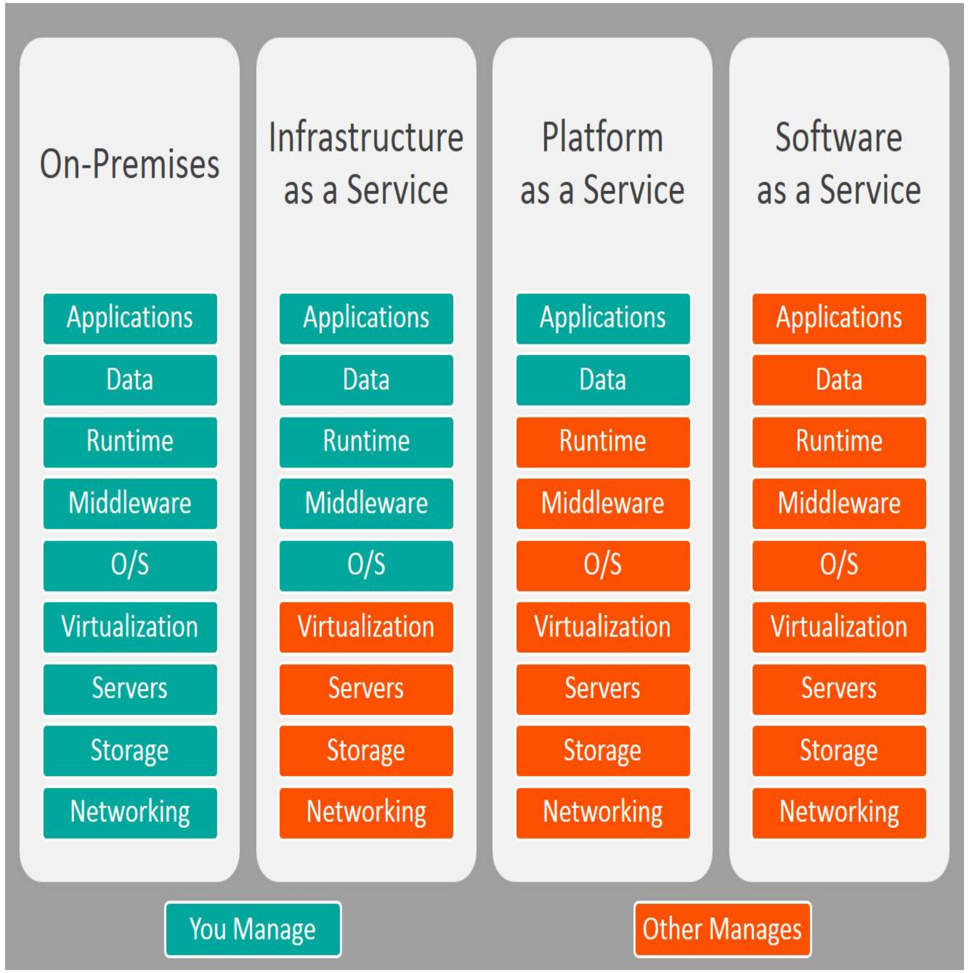
- Provides **virtual servers, storage, and networking**.
- You manage applications and operating systems; the provider manages the infrastructure.
- *Example:* Microsoft Azure VMs, AWS EC2, Google Compute Engine.

PaaS (Platform as a Service)

- Provides a **platform with tools** to develop, test, and deploy applications.
- Developers don’t worry about servers or OS; they just focus on coding.
- *Example:* Azure App Service, Google App Engine, AWS Elastic Beanstalk.

SaaS (Software as a Service)

- Ready-to-use **software applications** delivered over the internet.
- No installation needed; just log in and use.
- *Example:* Microsoft 365, Google Workspace, Zoom, Salesforce.



On-Premises	Infrastructure as a Service	Platform as a Service	Software as a Service
🟩 Applications	🟩 Applications	🟩 Applications	🟧 Applications
🟩 Data	🟩 Data	🟩 Data	🟧 Data
🟩 Runtime	🟩 Runtime	🟧 Runtime	🟧 Runtime
🟩 Middleware	🟩 Middleware	🟧 Middleware	🟧 Middleware
🟩 O/S	🟩 O/S	🟧 O/S	🟧 O/S
🟩 Virtualization	🟧 Virtualization	🟧 Virtualization	🟧 Virtualization
🟩 Servers	🟧 Servers	🟧 Servers	🟧 Servers
🟩 Storage	🟧 Storage	🟧 Storage	🟧 Storage
🟩 Networking	🟧 Networking	🟧 Networking	🟧 Networking

🟩 You Manage

🟧 Other Manages

TYPES OF CLOUD

Public Cloud

- Services are delivered over the **internet** and shared among multiple users.
- Cost-effective and scalable.
- *Examples:* Microsoft Azure, AWS, Google Cloud.

Private Cloud

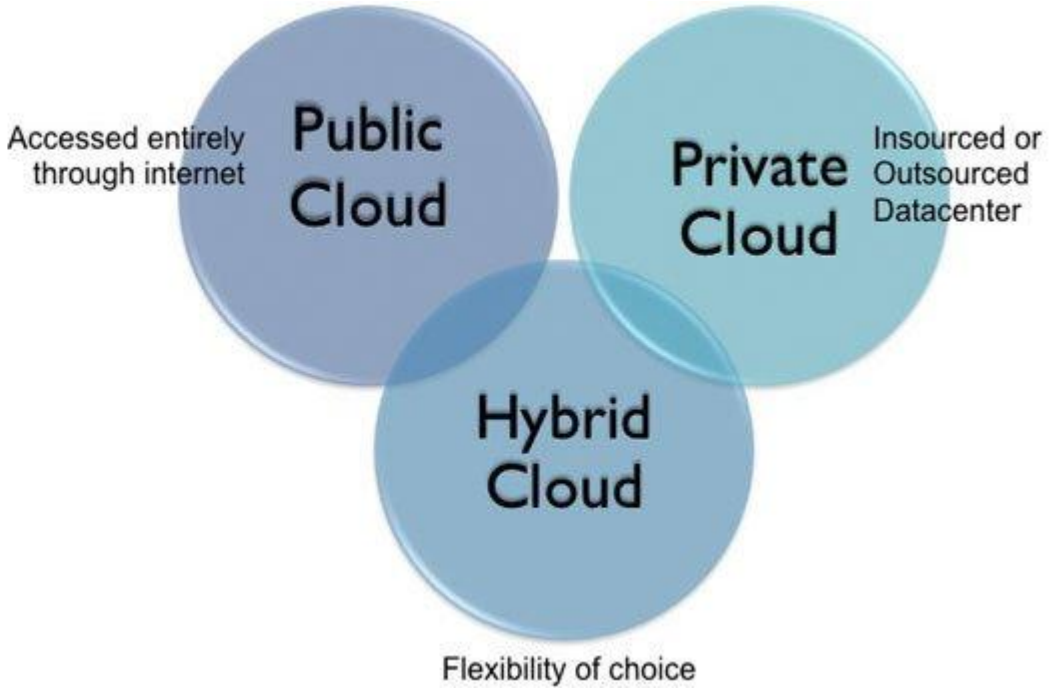
- Cloud infrastructure is dedicated to a **single organization**.
- Provides more control, customization, and security.
- *Example:* VMware Private Cloud, OpenStack.

Hybrid Cloud

- Combination of **Public + Private Cloud**.
- Organizations keep sensitive data in private cloud and use public cloud for scalability.
- *Example:* Azure Hybrid Solutions, AWS Outposts.

Multi-Cloud

- Using **multiple cloud providers** (e.g., AWS + Azure + GCP) at the same time.
- Avoids vendor lock-in and improves resilience.


Accessed entirely through internet
Public Cloud
Private Cloud
Insourced or Outsourced Datacenter
Hybrid Cloud
Flexibility of choice

Microsoft Azure Services / Resources

Azure provides a wide range of cloud services. The major categories are:

- **Compute Services**
  - Run applications, VMs, and containers.
  - *Examples:* Azure Virtual Machines, Azure Kubernetes Service (AKS), Azure Functions (Serverless).
- **Storage Services**
  - Store and manage structured & unstructured data.
  - *Examples:* Azure Blob Storage, Azure Files, Azure Disk Storage.
- **Networking Services**
  - Connect apps, users, and resources securely.
  - *Examples:* Azure Virtual Network (VNet), Load Balancer, Application Gateway, VPN Gateway, ExpressRoute.

Microsoft Azure Services / Resources

Database Services

- Fully managed relational & NoSQL databases.
- *Examples:* Azure SQL Database, Cosmos DB, Azure Database for MySQL/PostgreSQL.

Identity & Security Services

- Manage users, roles, and secure access.
- *Examples:* Azure Active Directory (Azure AD), Key Vault, Azure Security Center, Defender for Cloud.

AI & Machine Learning Services

- Build, train, and deploy AI models.
- *Examples:* Azure Cognitive Services, Azure Machine Learning, Bot Services.

DevOps & Developer Tools

- Continuous Integration/Continuous Deployment (CI/CD).
- *Examples:* Azure DevOps, GitHub Actions (integrated), Azure Pipelines.

Microsoft Azure Services / Resources

Analytics & Big Data Services

- Process, analyze, and visualize large datasets.
- *Examples:* Azure Synapse Analytics, Data Lake, HDInsight, Power BI.

IoT (Internet of Things) Services

- Connect, monitor, and manage IoT devices.
- *Examples:* Azure IoT Hub, IoT Central, Sphere.

Management & Monitoring Services

- Tools for governance, compliance, and monitoring.
- *Examples:* Azure Monitor, Log Analytics, Cost Management, Azure Policy.

Key Azure Cloud Terminologies

- **Tenant** – A dedicated instance of Azure Active Directory (Azure AD) for an organization.

- **Subscription** – Defines the **billing boundary** in Azure. All resources created in Azure are linked to a subscription.

- **Resource** – Any service you create in Azure (VM, Storage Account, Database, etc.).

- **Resource Group (RG)** – A **logical container** to organize and manage related resources together.

- **Management Group** – A higher-level container to organize **multiple subscriptions**.

Key Azure Cloud Terminologies

Region – A **geographical location** (like East US, Central India) where Azure data centers are located.

Availability Zone (AZ) – Physically separate data centers within a region for high availability.

Virtual Network (VNet) – Private network in Azure to securely connect resources.

Azure Active Directory (AAD) – Identity and access management service for users, apps, and devices.

Azure Marketplace – A store to find and deploy pre-built cloud solutions and apps.

Key Azure Cloud Terminologies

Azure Portal – The **web-based interface** to manage all Azure services.

Azure CLI / PowerShell – Command-line tools to create and manage Azure resources.

ARM (Azure Resource Manager) – The **deployment and management framework** for Azure resources.

Azure Policy – Service to enforce rules and compliance on resources.

Tags – Key-value pairs used for **organizing and cost-tracking** resources

Key Azure Cloud Terminologies

- **VM Scale Sets** – Auto-scaling group of virtual machines.
- **Load Balancer** – Distributes network traffic across multiple resources.
- **Azure Key Vault** – Securely stores keys, passwords, and secrets.
- **Azure Monitor** – Collects metrics and logs to monitor applications and infrastructure.
- **Pay-as-you-go** – The Azure pricing model where you only pay for what you use.

What is an Azure Subscription?

An **Azure Subscription** is a **logical container** that holds all your **resources** (like Virtual Machines, Storage, Databases, Networks, etc.) and defines the **billing boundary** for them.

Every resource you create in Azure must belong to a **subscription**.

It decides **how much you are billed** and helps in **managing access, policies, and compliance**.

You can have **multiple subscriptions** for different departments, projects, or environments (Dev, Test, Prod).

Role of subscription in Azure hierarchy

In Azure, everything is organized in a **hierarchical structure**:

Management Group → Subscription → Resource Group → Resources

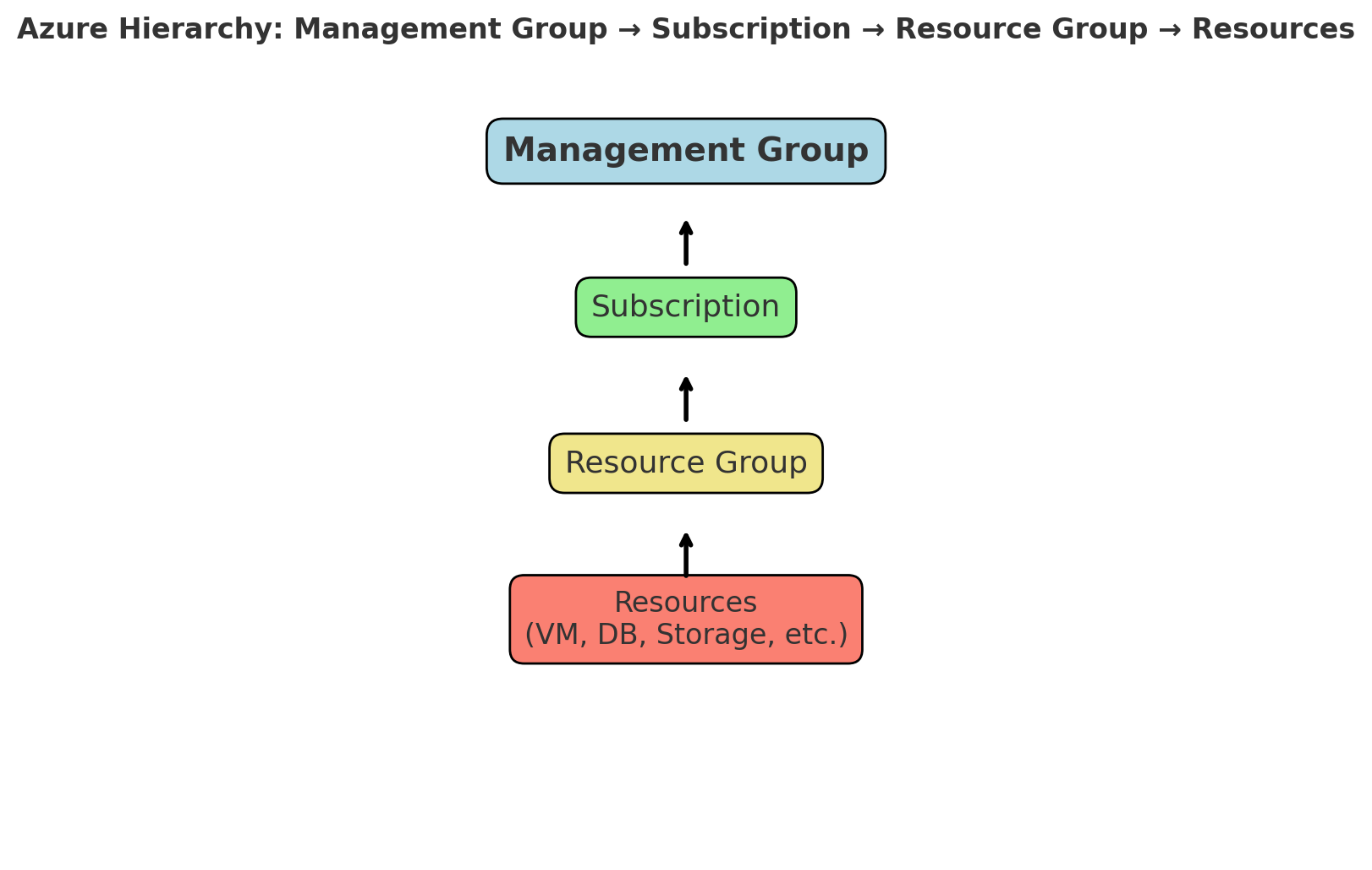
Management Group → Used to manage multiple subscriptions together with common policies and governance.

Subscription → Defines the **billing boundary**. All resources created in Azure must belong to a subscription. It also helps in **access control** and cost management.

Resource Group (RG) → A **logical container** inside a subscription to hold related resources (VMs, Databases, Storage, etc.).

Resources → The actual services you use (VM, Storage, App Service, etc.).

👉 The **Subscription** acts as the **bridge between governance (Management Groups)** and the **actual resources (RGs & Resources)**, ensuring proper **billing, security, and organization**.



Azure Hierarchy: Management Group → Subscription → Resource Group → Resources

Types of subscriptions (Free Trial, Pay-As-You-Go, Enterprise Agreement, Student)

TYPES OF AZURE SUBSCRIPTIONS

FREE TRIAL – GIVES LIMITED FREE CREDITS (E.G., $200 FOR 30 DAYS) TO EXPLORE AZURE SERVICES.

PAY-AS-YOU-GO – FLEXIBLE MODEL WHERE YOU **PAY ONLY FOR WHAT YOU USE** (NO UPFRONT COST).

ENTERPRISE AGREEMENT (EA) – FOR LARGE ORGANIZATIONS; OFFERS BULK PURCHASING, DISCOUNTS, AND CENTRALIZED BILLING.

STUDENT SUBSCRIPTION – FREE CREDITS AND SERVICES FOR STUDENTS, NO CREDIT CARD REQUIRED (WITH VALID STUDENT EMAIL).

Subscription Management

Creating and Managing Subscriptions

In Azure, a subscription is the starting point for using cloud services. You can easily create a new subscription through the Azure Portal and assign it to a department, project, or environment such as Development, Testing, or Production. Each subscription provides an isolated billing and management boundary, which makes it easier to control costs and permissions. Administrators can rename, disable, or even transfer subscriptions between accounts if needed, giving flexibility for organizational changes.

Linking Subscriptions to Azure Active Directory (Tenant)

Every Azure subscription is always tied to an **Azure Active Directory (Azure AD) tenant**. The tenant acts as the identity and access management system for the subscription. This means that all user logins, permissions, and role assignments within a subscription are controlled by Azure AD. By linking a subscription to a tenant, organizations ensure that resources are accessed only by authorized users. If required, subscriptions can also be moved between tenants, although this comes with certain limitations.

Setting up Billing and Payment Methods

Billing in Azure is handled at the subscription level. Once a subscription is created, you must set up a payment method such as credit card, debit card, or enterprise invoice (for large organizations). Azure also provides cost management tools to monitor spending. You can configure budgets, set up alerts when usage crosses a threshold, and analyze costs per service or department using tags. This ensures that organizations maintain visibility and control over their cloud expenses while avoiding unexpected bills.

Billing & Cost Management

Azure provides a clear **billing structure** where each subscription generates its own invoices containing usage details, services consumed, and applicable taxes. Through the **Cost Management + Billing** service in the Azure Portal, users can analyze spending trends, break down costs by service, resource group, or tags, and identify areas for optimization. The **Azure Pricing Calculator** helps estimate costs before deployment by comparing regions, VM sizes, and service tiers. To save costs, Azure offers features like **budgets and alerts** to control spending, **reserved instances** for long-term savings, auto-shutdown of idle resources, and the **Azure Hybrid Benefit** for reusing existing Windows and SQL licenses.

Access Control & Security

Azure provides strong **Access Control & Security** through **Role-Based Access Control (RBAC)**, which ensures that users and groups have only the permissions required to perform their tasks. RBAC uses built-in roles such as **Owner, Contributor, and Reader**, while also supporting custom roles for advanced scenarios. These roles can be **assigned at different scopes**—from the entire subscription down to specific resource groups or individual resources—allowing fine-grained control over access. For managing multiple users, **Azure Active Directory (Azure AD)** acts as the central identity and access service, enabling organizations to add users, groups, and service principals, and enforce security policies like **Multi-Factor Authentication (MFA)** and conditional access. This approach makes it easier to collaborate securely across teams while protecting sensitive resources, ensuring compliance, and reducing the risk of unauthorized access.

Policies & Governance

Azure helps organizations maintain control and compliance through its **Policies & Governance** features. **Azure Policy** allows you to enforce compliance rules by restricting resource types, locations, or configurations to meet organizational or regulatory standards. For large-scale governance, **Azure Blueprints** provide ready-made templates that bundle policies, role assignments, and resource groups, making it easier to deploy and manage environments consistently across multiple subscriptions. Additionally, **resource tagging** enables cost allocation, better organization, and easier management of resources by applying labels such as department, environment, or project. Together, these tools ensure that Azure environments remain secure, compliant, and well-governed.

Multiple Subscriptions

Organizations often use **multiple subscriptions** in Azure to separate environments (such as development, testing, and production), manage costs by department or project, or meet compliance and billing requirements. To simplify administration, Azure provides **Management Groups**, which allow you to organize multiple subscriptions under a single hierarchy, apply governance policies, and manage access consistently across all subscriptions. Additionally, Azure supports **cross-subscription resource access**, enabling services in one subscription to securely communicate with resources in another through role assignments, virtual network peering, or shared resource configurations. This approach ensures flexibility, better cost control, and strong governance for enterprises operating at scale.

Monitoring & Alerts

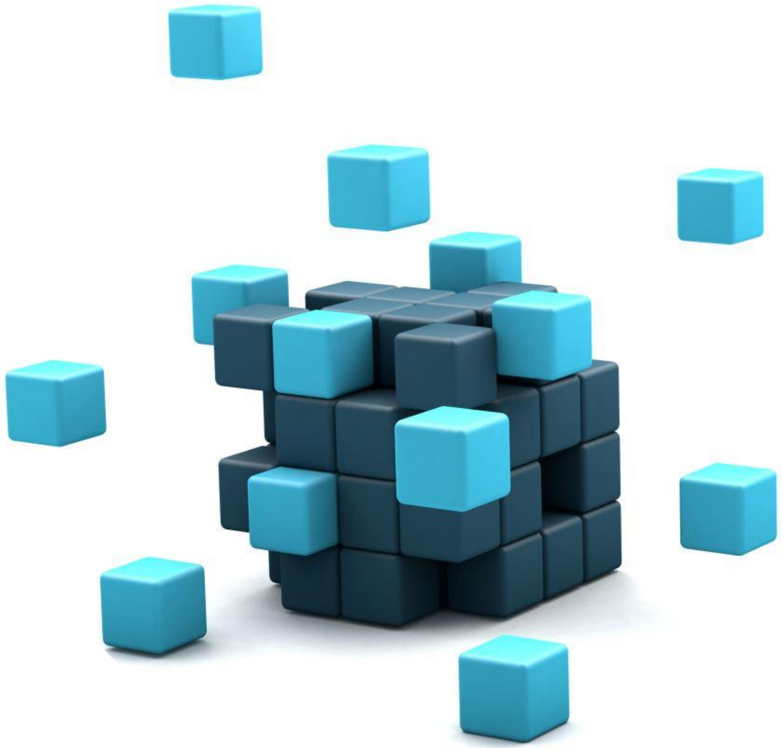
Azure provides built-in tools for **Monitoring & Alerts** to help track usage, performance, and security. At the subscription level, **Azure Monitor** can be set up to collect metrics and logs across all resources, giving a centralized view of health and performance. Users can configure **budget alerts** in Cost Management to receive notifications when spending approaches or exceeds defined thresholds. The **Activity Log** records all management operations, showing who performed which action and when, enabling transparency, auditing, and quick troubleshooting of issues.

What is a Management Group?

A **Management Group** in Azure is a **container that helps you organize and manage multiple subscriptions together**.

- It sits **above subscriptions** in the Azure hierarchy.
- Useful for applying **governance, policies, and access control** consistently across many subscriptions.
- You can create a hierarchy of management groups (like departments → projects → teams) to mirror your organization's structure.
- All subscriptions under a management group **automatically inherit** the policies and access controls applied at the group level.

Example:
If a company has 10 subscriptions for Finance, HR, and IT, instead of applying a security policy to each one individually, they can attach all those subscriptions to a **Finance Management Group** and enforce the policy once.



List of Management Group

Yes, in Azure, a **Management Group** can contain a **list of subscriptions** or even **child management groups**. This allows organizations to build a hierarchy that matches their structure (for example, company → departments → projects).

- When you place subscriptions inside a management group, all the **policies, RBAC permissions, and compliance rules** applied at the management group level are **inherited automatically** by every subscription under it. This makes it easier to manage security, governance, and cost control across multiple subscriptions in a large enterprise.

Example:

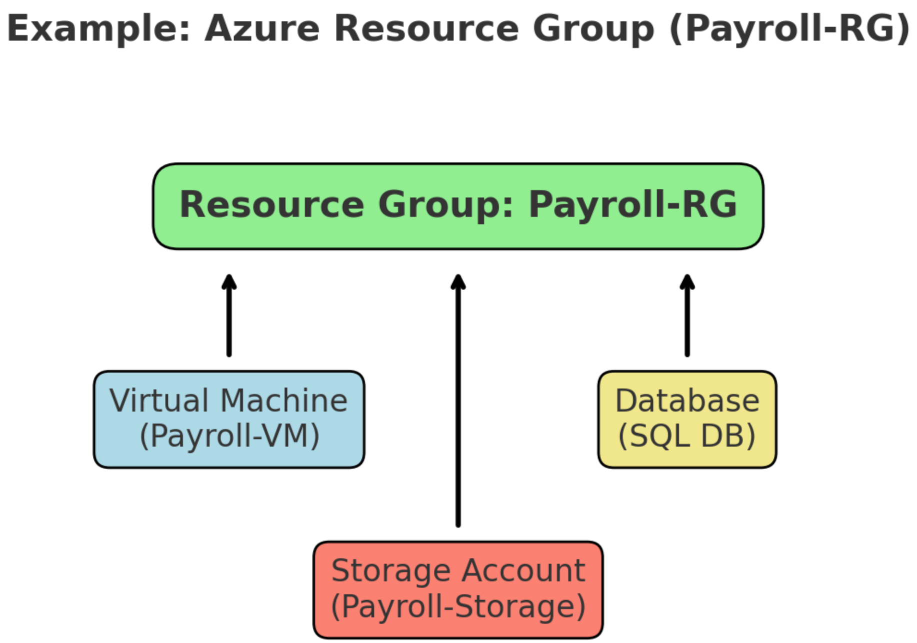
- A company creates a **Finance Management Group**. Inside it, they keep subscriptions for **Payroll** and **Accounting**.
- Any rule applied at the Finance Management Group level (like encryption or region restriction) will apply to both subscriptions without needing to set them individually.

What is a Resource Group?

A **Resource Group (RG)** in Azure is a **logical container** that holds related resources for an application, project, or workload. All the resources inside a Resource Group share the same **lifecycle, permissions, and management policies**.

- Every resource in Azure (VM, Storage, Database, Network, etc.) must belong to a **Resource Group**.
- You can **deploy, manage, and delete** resources as a group. For example, deleting the Resource Group deletes all resources inside it.
- Helps in **organizing resources** based on environment (Dev, Test, Prod), department (HR, IT, Finance), or project.
- Supports **RBAC (Role-Based Access Control)** and **tagging** for cost tracking and governance.

Example:
If you create a Payroll Application, you can keep its **VM, Database, and Storage Account** all inside one Resource Group named *Payroll-RG*.



Example: Azure Resource Group (Payroll-RG)

Resource Group: Payroll-RG
Virtual Machine (Payroll-VM)
Storage Account (Payroll-Storage)
Database (SQL DB)

In Azure, a **Resource Group (RG)** is like a **folder** where you keep all related resources for a project or application. For example, in the diagram, the **Payroll-RG** contains a **Virtual Machine**, a **Database**, and a **Storage Account**. By grouping them together, you can manage, monitor, and even delete them as a single unit. This makes it easier to **organize, secure, and control costs** for applications in Azure.

What are Resources in Azure?

In Azure, a **Resource** is the **basic building block** — any service or component you create and use inside the cloud.

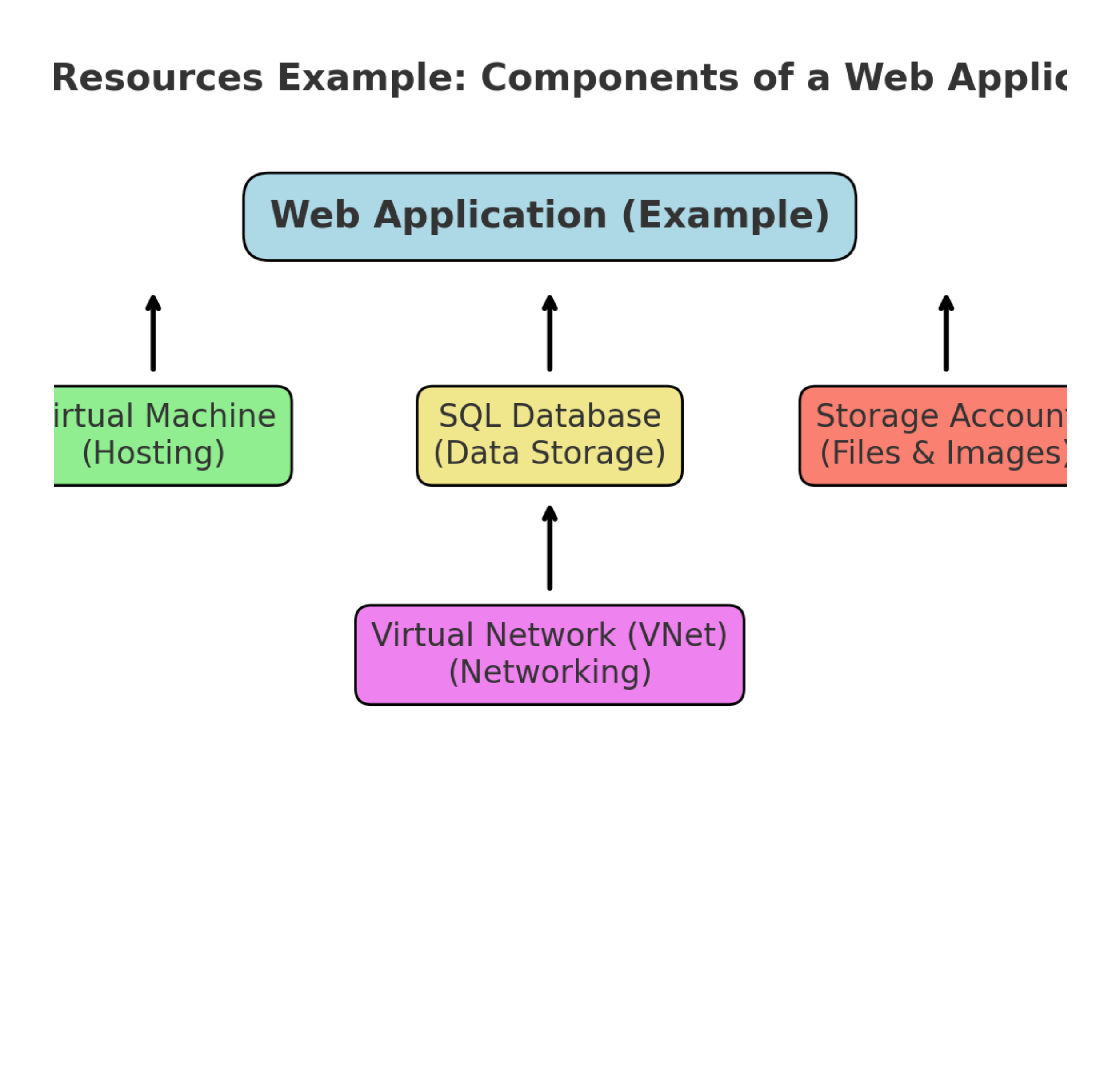
Examples of resources: **Virtual Machine (VM)**, **Storage Account**, **SQL Database**, **Virtual Network (VNet)**, **Key Vault**, **App Service**, etc.

- Every resource must belong to a **Resource Group** and a **Subscription**.
- Resources can be managed individually or as part of a group (for easier lifecycle management).
- You can assign **tags, permissions, and policies** to resources for better organization and governance.

Example:
If you build a web application on Azure, the resources could be:

- A **VM** for hosting,
- A **Database** for storing data,
- A **Storage Account** for images,
- A **VNet** for networking.

In Azure, **resources** are the actual services that make up your application. For example, a web application may use a **Virtual Machine** for hosting, an **SQL Database** for storing user data, a **Storage Account** for saving files and images, and a **Virtual Network (VNet)** for secure communication. Each of these is a separate **resource**, but together they work as one complete solution inside Azure.


Resources Example: Components of a Web Applic
Web Application (Example)
irtual Machine
(Hosting)
SQL Database
(Data Storage)
Storage Accoun
(Files & Images
Virtual Network (VNet)
(Networking)