Understanding the **fundamentals of IAM (Identity and Access Management)** in Azure—or any cloud environment—is crucial for securing resources and managing who can do what. Here's a breakdown of the key IAM components:

🧠 IAM Fundamentals: Users, Roles, Permissions

1. 👤 Users (Identities)

Users represent individuals or entities that interact with Azure resources. They can include:

Type	Description
User Accounts	Real human users (e.g., alice@contoso.com).
Groups	A collection of users (Azure AD groups) to simplify management.
Service Principals	App identities used by applications or services.
Managed Identities	Automatically managed identities for Azure services.

---

2. 🧱 Roles

A **role** is a collection of **permissions** that define what actions an identity can perform on Azure resources.

Type	Description
Built-in Roles	Predefined roles like Reader, Contributor, Owner, etc.
Custom Roles	User-defined roles tailored to specific needs.

📌 Examples of Built-in Roles:

Role Name	Permissions
Reader	View resources only

Contributor	Manage everything except access permissions
Owner	Full control including assigning roles
User Access Administrator	Manage access, not resources

---

3. 🔑 Permissions

Permissions define **what actions** are allowed. Each role contains a list of actions in the form of **Azure Resource Manager (ARM) operations**, like:

- `Microsoft.Compute/virtualMachines/read` – View a VM
- `Microsoft.Compute/virtualMachines/write` – Modify a VM
- `*/read` – Read all resources
- `Microsoft.Authorization/*/write` – Assign roles (RBAC permissions)

🔄 Relationship Between Users, Roles, and Permissions

Access Assignment = User + Role + Scope

Element	Example
User	`alice@contoso.com`
Role	`Contributor`
Scope	Subscription, Resource Group, or specific resource

➡️ This determines **what Alice can do and where** she can do it.

🔁 Scope Levels in Azure IAM

Scope Level	Description
Management Group	Highest level (can manage multiple subscriptions)
Subscription	Container for billing and resources
Resource Group	Logical container for related resources
Resource	Individual Azure service (e.g., VM, Storage Account)

🔽 **Access is inherited**: If assigned at the subscription level, permissions apply to all child resources.

🛠️ How to Assign Roles (Portal Example)

1. Navigate to the **resource** (or RG, subscription).
2. Go to **Access Control (IAM)**.
3. Click **+ Add > Add Role Assignment**.
4. Select the **role**, and assign it to a **user, group, or service principal**.

✅ Summary Table

Concept	What it Defines
User	Who is accessing
Role	What they can do
Permission	Specific actions allowed
Scope	Where they can do it
