Interpreting **access assignments in Azure** means understanding **who** has **what permissions**, **where**, and **how** those permissions are granted. Azure uses **Role-Based Access Control (RBAC)** to handle this.

🔍 What Is an Access Assignment in Azure?

An **access assignment** in Azure is when a **role** is assigned to a **security principal** (user, group, service principal, or managed identity) at a **scope** (management group, subscription, resource group, or resource).

📘 Components of an Access Assignment

Element	Description
Security Principal	Who is getting access (user, group, SP, managed identity)
Role Definition	What permissions they have (e.g., Reader, Contributor)
Scope	Where the permissions apply (e.g., Subscription X, Resource Group Y)

🧭 How to View Access Assignments

✅ Azure Portal:

1. Navigate to a **resource**, **resource group**, or **subscription**.
2. Click **Access Control (IAM)**.
3. Go to the **Role assignments** tab.
4. You will see:
    - **Name** (who has access)
    - **Role** (what they can do)

- **Scope** (where it's applied)
- **Type** (user, group, service principal)

✅ Azure CLI:

az role assignment list --all --output table

For a specific user:

az role assignment list --assignee <userPrincipalName>

✅ PowerShell:

Get-AzRoleAssignment

For a specific user:

Get-AzRoleAssignment -SignInName user@domain.com

🧠 How to Interpret Role Assignments

Let's break it down with an example.

🔸 Example Access Assignment

Name	Role	Scope	Type
`alice@contoso.com`	Contributor	Subscription: `Contoso-Prod`	User

Interpretation:

- **Alice** has **Contributor** access to everything within the **Contoso-Prod subscription**.
- She can **create, delete, and manage** resources, but **not assign roles** to others.
- The access is **directly assigned** (not via group).

🧩 Other Scenarios

🔹 **Group-Based Assignment**

Name	Role	Scope	Type
`DevOps-Team`	Contributor	Resource Group: `RG-App`	Group

Interpretation: All users in the **DevOps-Team group** have **Contributor** access to the `RG-App` resource group.

🔹 **Service Principal Assignment**

Name	Role	Scope	Type
`app-service-sp`	Reader	Subscription X	Service Principal

Interpretation: The service principal used by an application has **read-only** access to Subscription X.

✅ Tips for Interpreting Access

- **Look at inherited scopes**: Assignments at higher levels (management group or subscription) apply to all child resources.
- **Check group memberships**: Users might have access via **Azure AD groups**, not directly.
- **Use the "Check access" feature** in the Portal to see **effective permissions**.

🔐 Common Built-in Roles and Their Meaning

Role	Permissions

Reader	View resources only
Contributor	Create/manage all resources except RBAC
Owner	Full control including assigning roles
User Access Administrator	Can manage access (RBAC) but not resources

---

🛠️ Tools to Help

- **Microsoft Entra ID**: See group memberships and directory roles.
- **Access Reviews**: Audit and clean up role assignments.
- **PIM (Privileged Identity Management)**: View and manage just-in-time access.
