**RBAC**

**1. Introduction to RBAC in Azure**

**What is RBAC?**

**RBAC (Role-Based Access Control) is a system in Azure that controls who can access what by assigning specific roles to users, groups, or applications. It helps enforce the principle of least privilege, meaning users should have only the permissions they need to perform their tasks.**

**Why is RBAC Important?**

* **Security: Prevents unauthorized access.**
* **Control: Allows fine-grained access management.**
* **Compliance: Helps organizations follow security policies.**

**2. RBAC Basics: Key Concepts**

**2.1. Identity Types in Azure**

**Before assigning permissions, you must understand who can receive permissions in Azure:**

1. **Users: Human identities (e.g., you, an admin, a developer).**
2. **Groups: A collection of users (e.g., "Developers Group").**
3. **Service Principals: Used by applications to access Azure.**
4. **Managed Identities: Special accounts managed by Azure for automation.**

**2.2. Understanding Roles**

**A role in Azure is a set of permissions that define what an identity can do.**

**Built-in Roles**

**Azure provides predefined roles for common use cases. Some important ones:**

1. **Owner – Full access, including assigning roles.**
2. **Contributor – Can create and manage resources but cannot assign roles.**
3. **Reader – Can view resources but cannot modify them.**
4. **Storage Blob Data Reader – Can read blob data inside a Storage Account.**
5. **Storage Blob Data Contributor – Can read, write, and delete blob data but cannot manage the Storage Account itself.**

**Custom Roles**

**If built-in roles don't meet your needs, you can create custom roles with specific permissions.**

**2.3. Understanding Scope in RBAC**

**RBAC assigns permissions at different levels, called scopes. A scope defines where the permissions apply.**

| **Scope Level** | **Example** | **Effect** |
| --- | --- | --- |
| **Subscription** | **Sub-12345** | **Permissions apply to all resources in the subscription.** |
| **Resource Group** | **RG-Sales** | **Permissions apply only to resources in this group.** |
| **Resource** | **StorageAccount01** | **Permissions apply only to this specific resource.** |

**👉 Lower-level scopes override higher-level scopes.  
Example: If you are a Contributor at the Resource Group level, you cannot delete a subscription.**

**3. RBAC Hands-on Example: Contributor vs. Storage Blob Data Contributor**

**Now, let’s deep dive into two roles to understand the difference.**

**3.1. Contributor Role (Control Plane Access)**

**Permissions**

**✅ Can create, update, and delete Azure resources.  
❌ Cannot access the data inside the resources.**

**Example**

**Imagine you are given Contributor access at the Storage Account level.**

* **You CAN create a Storage Account. ✅**
* **You CAN create a container inside the Storage Account. ✅**
* **You CANNOT upload, download, or view files (blobs) inside the container. ❌**

**👉 Contributor can manage the resource but not the data inside it!**

**3.2. Storage Blob Data Contributor Role (Data Plane Access)**

**Permissions**

**✅ Can read, write, and delete blob data inside a storage account.  
❌ Cannot manage the Storage Account itself.**

**Example**

**Imagine you are given Storage Blob Data Contributor access only on a container.**

* **You CAN upload a file to the container. ✅**
* **You CAN download and delete blobs inside the container. ✅**
* **You CANNOT create or delete the Storage Account. ❌**

**👉 Storage Blob Data Contributor can access the data but not the resource settings!**

**4. Key Concept: Control Plane vs. Data Plane**

**Azure permissions are divided into two levels:**

| **Type** | **What it Controls?** | **Example Roles** |
| --- | --- | --- |
| **Control Plane** | **Managing Azure resources** | **Owner, Contributor** |
| **Data Plane** | **Accessing data inside resources** | **Storage Blob Data Reader, Storage Blob Data Contributor** |

**🚀 Think of it this way:**

* **The Contributor is like a Storage Admin – they can manage the storage account but not access the data inside.**
* **The Storage Blob Data Contributor is like a File Manager – they can read, write, and delete files but not configure the storage account.**

**5. Step-by-Step Hands-On Practice**

**Scenario**

**You want to test how Contributor and Storage Blob Data Contributor roles work.**

**Step 1: Create a Storage Account**

1. **Go to Azure Portal → Search for Storage Accounts.**
2. **Click Create and fill in the details.**
3. **Once created, go to Containers → Click + Container → Name it test-container.**

**Step 2: Assign the Contributor Role**

1. **Go to your Storage Account → Access Control (IAM).**
2. **Click Add Role Assignment → Choose Contributor.**
3. **Assign this role to User 1 (or your test account).**
4. **Sign in as User 1 and test:**
   * **Can you create a container? ✅ (Yes)**
   * **Can you upload files inside the container? ❌ (No)**

**Step 3: Assign the Storage Blob Data Contributor Role**

1. **Go to your Storage Account → Containers → Select test-container.**
2. **Access Control (IAM) → Add Role Assignment.**
3. **Select Storage Blob Data Contributor.**
4. **Assign this role to User 2 (or your test account).**
5. **Sign in as User 2 and test:**
   * **Can you upload files inside the container? ✅ (Yes)**
   * **Can you create a container? ❌ (No)**

**6. Summary & Key Takeaways**

| **Role** | **Can Create Storage Account?** | **Can Configure Storage Account?** | **Can Upload/Download Blobs?** |
| --- | --- | --- | --- |
| **Contributor** | **✅ Yes** | **✅ Yes** | **❌ No** |
| **Storage Blob Data Contributor** | **❌ No** | **❌ No** | **✅ Yes** |

* **Contributor manages the Storage Account but cannot access data.**
* **Storage Blob Data Contributor manages data inside the Storage Account but cannot configure settings.**
* **Control Plane (managing resources) and Data Plane (accessing data) are separate in Azure.**

**ACCESSS CONTROL LIST(ACL)**