Azure User Management and RBAC

## **Background**

There is always requirement of giving employees the exact permissions they need. Unrestricted higher privileges can expose an account to attackers, and few permissions means that employees can’t get their work done efficiently. Azure helps to address this problem by offering fine-grained access management called Role-Based Access Control (RBAC).

## **What is RBAC (Role Based Access Control)?**

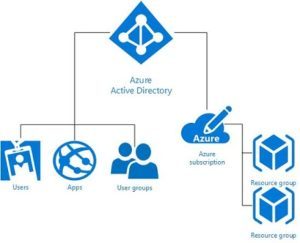
Azure Role-Based Access Control (RBAC) enables fine-grained access management for Azure. You can grant only the amount of access that users need to perform their task.

Using RBAC, you can segregate duties within your team and grant only the amount of access to users that they need to perform their jobs. Instead of giving everybody unrestricted permissions in your Azure subscription or resources, you can allow only certain actions. For example, use RBAC to let one employee manage web app as owner, while another can just perform read operations.

## **How Azure Access Management work?**

Azure subscription is associated with Azure Active Directory (AAD) directory. You can create users, groups in AAD and associate applications to AAD. You can assign access rights to any azure resource using the Azure portal, Azure command-line tools, and Azure Management APIs.

You can grant access by assigning the appropriate RBAC role to users, groups, and application. Permission can be given at a subscription, a resource group, or a single resource level.

Basic components of RBAC

## **How to add users to AAD in Azure Subscription?**

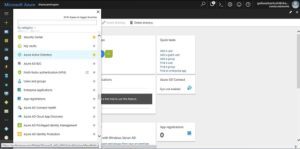
To provide permissions on azure resources like web app, you need to have users available in Azure environment.

Users in Azure are stored in Azure Active Directory; there are multiple ways to add users to AAD.

1. You can import users of on-premises Active Directory  
2. You can manually add user to AAD from Azure Portal  
3. You can add users using AAD B2C option.

For this article I am opting for option to add users manually in AAD.

Step 1: Navigate to Azure Active Directory from left menu.  
Azure Active Directory is multi-tenant cloud based directory and identity management service. As an administrator you can manage users, passwords, groups, applications in AAD.

Azure Active Directory

Step 2: Click on add user link and provide required permissions for the user at subscription level.

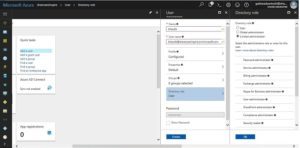
Access provided at subscription gets cascaded down till resources level, in following hierarchy.

1. Each subscription in Azure belongs to only one directory.  
2. Each resource group belongs to only one subscription.  
3. Each resource belongs to only one resource group.

e.g. Access that you grant at parent scopes is inherited at child scopes.

1. You assign the Reader role to an Azure AD group at the subscription scope. The members of that group can view every resource group and resource in the subscription.

2. You assign the Contributor role to an application at the resource group scope. It can manage resources of all types in that resource group, but not other resource groups in the subscription.

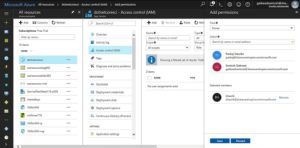
Permissions at Subscription level

## **How to provide permissions at resource level (e.g. Web App)?**

You can manage permission at subscription level, resource group level and at resource level too.

Let’s see how we can provide permissions to users at resource level (e.g. web app)

Navigate to web app properties in Azure dashboard, Select access control (IAM) property, this property enables you to view and edit existing permissions and enables to add users and provide new permissions to them. On selection of IAM property, azure opens new blade which enables user to add permissions, you can add desired users and provide required permissions on resource (in this case web app).

Permissions at Resource level

Azure RBAC has three basic roles that apply to all resource types:

Owner has full access to all resources including the right to delegate access to others.

Contributor can create and manage all types of Azure resources but can’t grant access to others.

Reader can view existing Azure resources.