**AZURE ACTIVE DIRECTORY**

1. Azure AD is nothing but an identity store in Azure. Here we can define users, groups, applications, and service principles. These users can authenticate onto Azure and they can access resources that are part of Azure subscription.
2. We can assign Azure AD roles to a user and these permissions are normally given to manage the various aspects of Azure AD.

**ROLE-BASED ACCESS CONTROL**

Role-based access control (RBAC) is meant to authorize a user to use resources in Azure.

So for example, you could give a role for a user to go ahead and give them the ability to create a storage account or to manage resource groups.

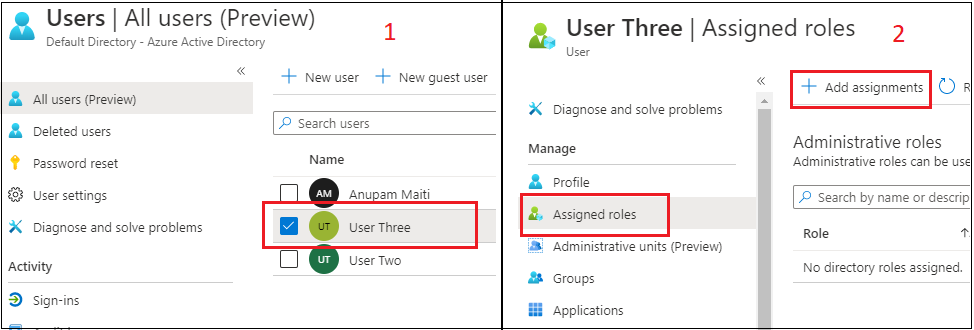
Role-based access control can be given at the management group level, subscription level, resource group level, or at the resource level.

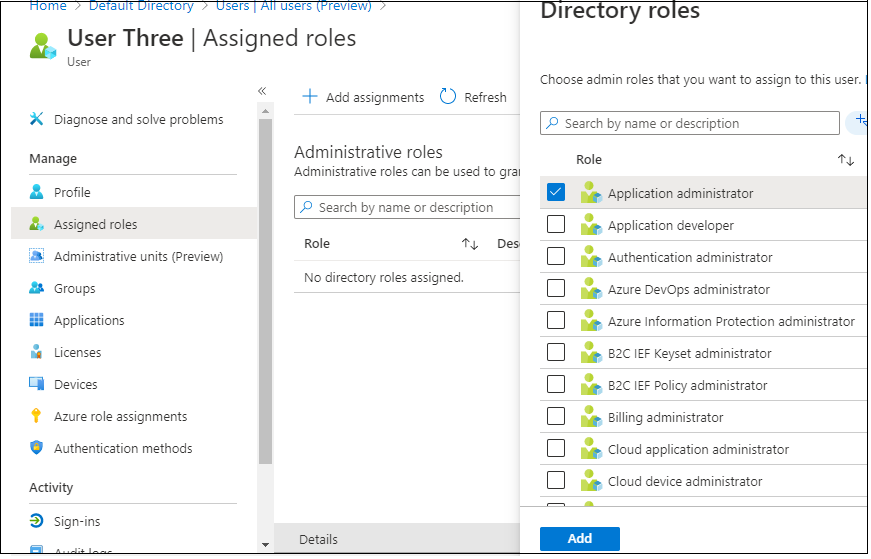
RBAC has three basic roles that apply to all resource types:

* *Owner*  
  This role has full access to all the resources and can delegate access to others.
* *Contributor*  
  This role can create and manage all types of resources, but can’t grant access to other users and groups.
* *Reader*  
  This role can view existing Azure resources.

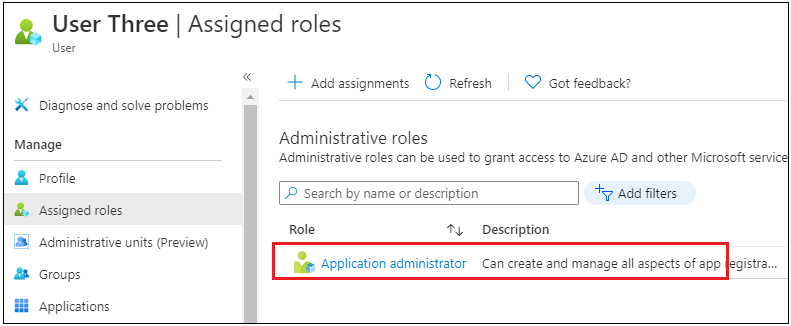
Assigning Azure AD Roles

Go to Azure Active Directory, and go to the Users section => click on a user for whom you want to add an AD Role. Now we can Assign roles for the user => Click on Assigned Role => + Add assignments.





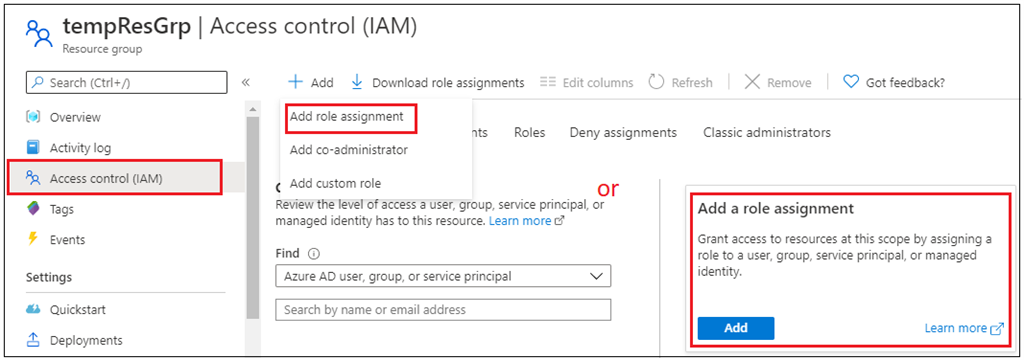
You will then see the role assigned to the user.



Assigning Role-Based Access Control

As we know, RBAC is used to give access to resources in Azure. Let's say you want to give RBAC access to a user for Resource Group.

Go to go Resource Group and click on the Access Control (IAM) option



Now click on the Add role assignment. In the next screen, you have to choose the Role to assign, and the principal to assign it to.

First, you can choose a Role, then choose access assign to, the last search for the user, and select. Once the user is selected, click on Save.

Azure AD roles are used to manage access to Azure AD resources, whereas Azure roles are used to manage access to Azure resources.

* The scope of Azure AD roles is at the tenant level, whereas the scope of Azure roles can be specified at multiple levels including management group, subscription, resource group, resource.
* I hope you found this information useful!

# Access and identity options for Azure Kubernetes Service (AKS)

You can authenticate, authorize, secure, and control access to Kubernetes clusters in a variety of ways.

* Using Kubernetes role-based access control (Kubernetes RBAC), you can grant users, groups, and service accounts access to only the resources they need.
* With Azure Kubernetes Service (AKS), you can further enhance the security and permissions structure via Azure Active Directory and Azure RBAC.

**Kubernetes RBAC**

Kubernetes RBAC provides granular filtering of user actions. With this control mechanism:

* You assign users or user groups permission to create and modify resources or view logs from running application workloads.
* You can scope permissions to a single namespace or across the entire AKS cluster.
* You create *roles* to define permissions, and then assign those roles to users with *role bindings*.
* To grant permissions across the entire cluster or to cluster resources outside a given namespace, you can instead use ClusterRoles.
* A ClusterRole grants and applies permissions to resources across the entire cluster, not a specific namespace.