RBAC Policy For Managing Role Assignments

The following topics will be covered in this document:

- Role-based access control (RBAC)
- RBAC access configuration
- Custom RBAC role

We will discuss RBAC implementation in this chapter and see how we can use it in our organization to put control for anonymous access.

1- Role-based access control (RBAC)

“Role-based access control helps you to manage and provide access to your resources with the restricted manner.”

Let us say in your organization the support team, application team, DB team, and so on are using the same subscription and there could be a possibility that if you allow everyone access to subscriptions, then there might be some changes mistakenly performed by any of the team members.

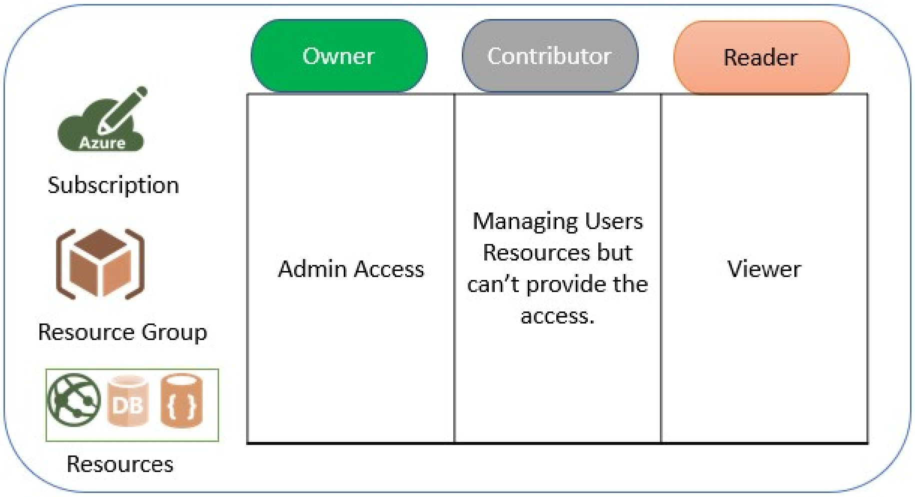
It could result in a disruptive impact on the existing environment/subscription (production or non-production).

Hence, thinking of all such scenarios MS Azure has come up with a solution called **RBAC policy** which helps you to control the access. Let us say if you want to allow the DB team to access only DB resources which can be possible only through RBAC.

The DB team can only see the DB resources and cannot make the changes to other services. So, using RBAC, you can control the access.

As per MS Azure recommendation, the best practice that you can provide is the least role access which will help the user to provide the exact access which he needs. RBAC can be applied to groups, applications or resources, and so on.

For any services, there are built-in RBAC roles defined as shown in the following diagram:



Owner	The owner will have complete access of all your resources or specific resources just like the admin of your subscription.
Contributor	The contributor will have equal access like the owner but cannot provide access to resources or at the subscription level. However, he can create and manage the resources.
Reader	In the reader role, a user will have access to read or view permission to specific resources or subscriptions. However, he is not allowed to change or create any new resources.
User access administrator	The user access administrator will help you to manage user access to Azure resources.

2- RBAC access configuration

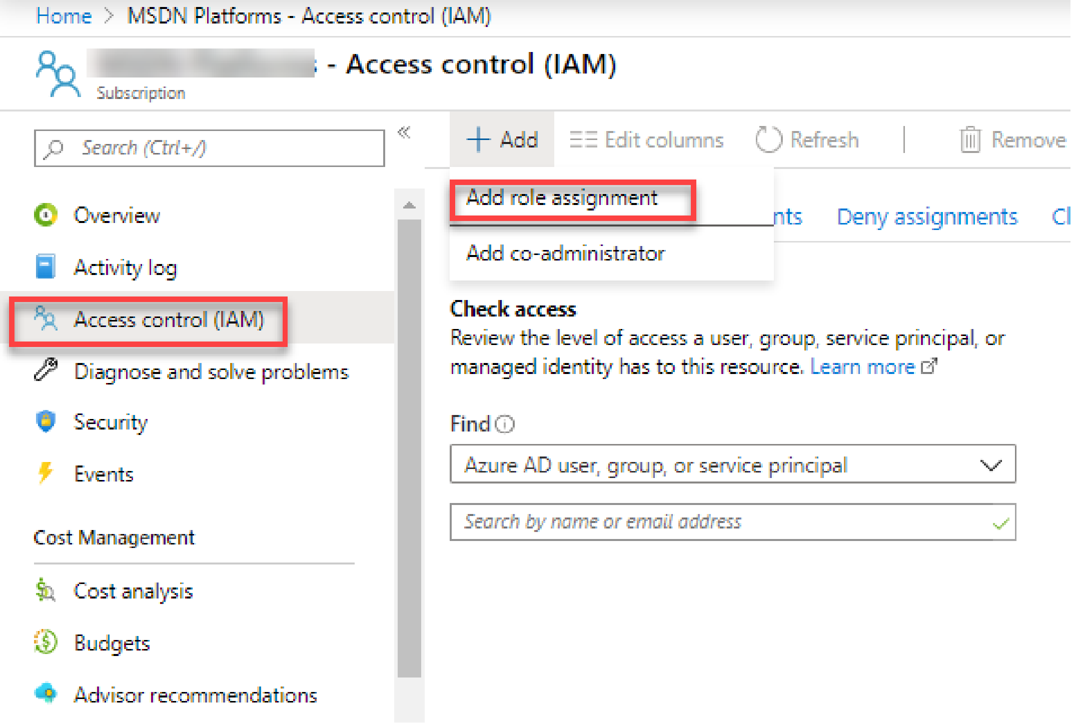
RBAC access can be configured from various types like Azure resources, Azure subscriptions, and Azure resources group as well. In this section, we will see how to implement those scenarios using RBAC.

2.1- Subscription access using the RBAC policy

We will learn how to provide access to subscriptions as per the organization policy.

1. Go to the **Subscription** option.

2. Click on **Access control (IAM)** as highlighted in the following picture and select **Add role assignment**:



Home > MSDN Platforms - Access control (IAM)

[redacted] - Access control (IAM)

Subscription

Check access

Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

Find: Azure AD user, group, or service principal

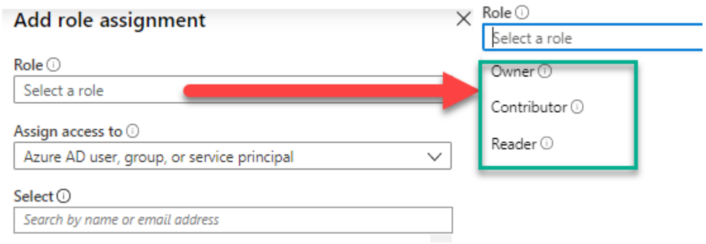
Search by name or email address

3. Once you click on **Add role assignment**:

1. Select the **Owner**, **Contributor**, or **Reader** role as per your

requirements.

2. Type and search the user ID for which you want to provide the access as shown in the following screenshot:



Add role assignment

Role

Select a role

Assign access to

Azure AD user, group, or service principal

Select

Search by name or email address

Role

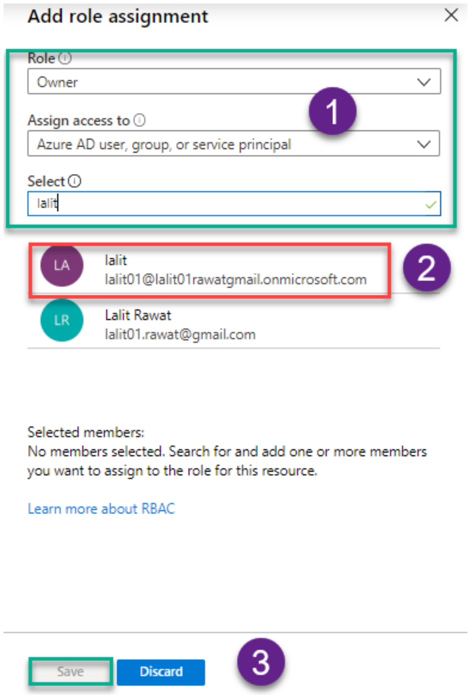
Select a role

Owner

Contributor

Reader

4. When you select all the required details, your screen will look like the following screenshot. Click on the **Save** button to apply the changes. Once done, the user will be able to log in to the subscription and access the resources:



Add role assignment

Role: Owner

Assign access to: Azure AD user, group, or service principal

Select: lalit

LA lalit lalit01@lalit01rawatgmail.onmicrosoft.com

LR Lalit Rawat lalit01.rawat@gmail.com

Selected members:
No members selected. Search for and add one or more members you want to assign to the role for this resource.

Learn more about RBAC

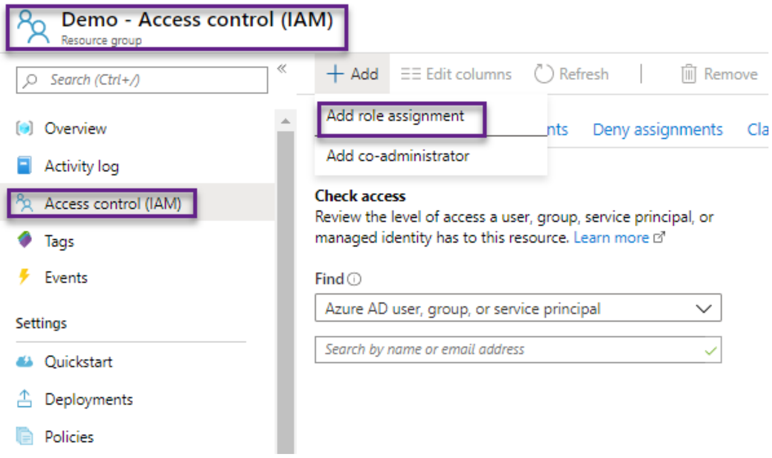
In this section, we learned how to assign the RBAC roles at the subscription level.

2.2- Resource group access using the RBAC policy

We will learn how to provide access to the resources group as per the organization policy.

1. Go to the **Resource group** option.

2. Click on **Access control (IAM)** and select **Add role assignment** as shown in the following screenshot:



Check access

Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

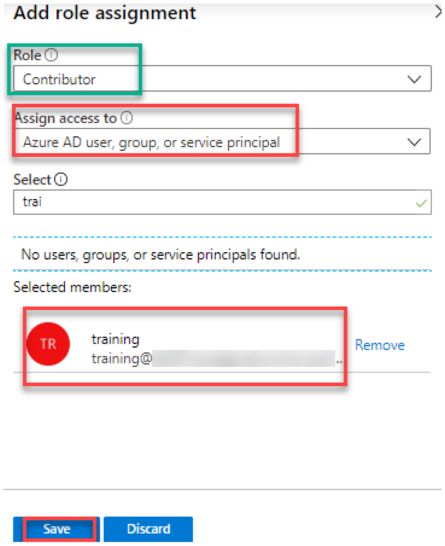
Find: Azure AD user, group, or service principal

Search by name or email address

3. Once you click on **Add role assignment**:

1. Select the **Owner**, **Contributor**, or **Reader** role as per your requirements.
2. Type and search the user ID for which you want to provide the access.
3. Once you select all the required details, your screen will look like the following screenshot. Click on the **Save** button to apply the changes.

4. Once done, the user will be able to see the resource group and its resources which reside in the resource group:



Add role assignment

Role ⓘ

Contributor

Assign access to ⓘ

Azure AD user, group, or service principal

Select ⓘ

trai

No users, groups, or service principals found.

Selected members:

TR training
training@[redacted]

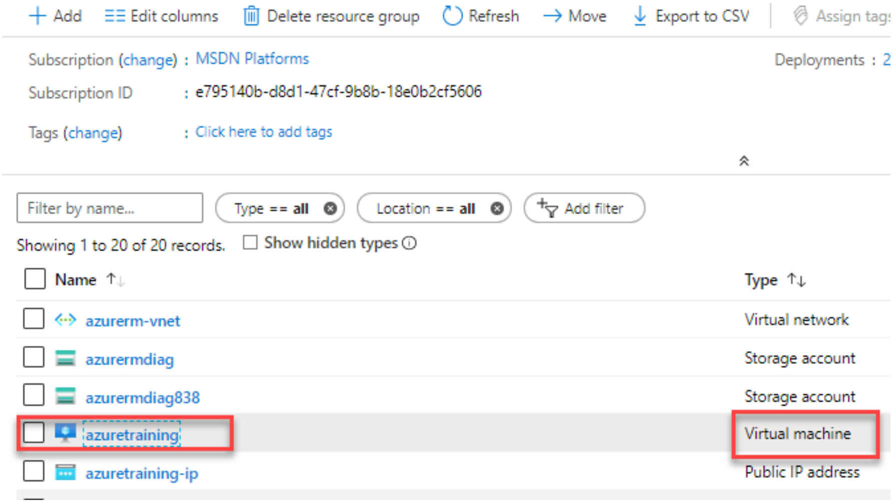
In this section, we learned how to assign the RBAC roles at the resource group level.

2.3- Resource access using the RBAC policy

We will learn how to provide access to resources like **Virtual Machines (VMs)**, DB, and so on as per the organization policy.

1. Go to the resource for which you would like to provide access like VM, DB WebApps, and so on.

2. Click on **Access control (IAM)** and select **Add role assignment**:



Subscription (change) : MSDN Platforms

Deployments : 2

Subscription ID : e795140b-d8d1-47cf-9b8b-18e0b2cf5606

Tags (change) : Click here to add tags

Showing 1 to 20 of 20 records. □ Show hidden types ⓘ

□ Name	Type
□ azurerm-vnet	Virtual network
□ azurermdiag	Storage account
□ azurermdiag838	Storage account
□ azuretraining	Virtual machine
□ azuretraining-ip	Public IP address

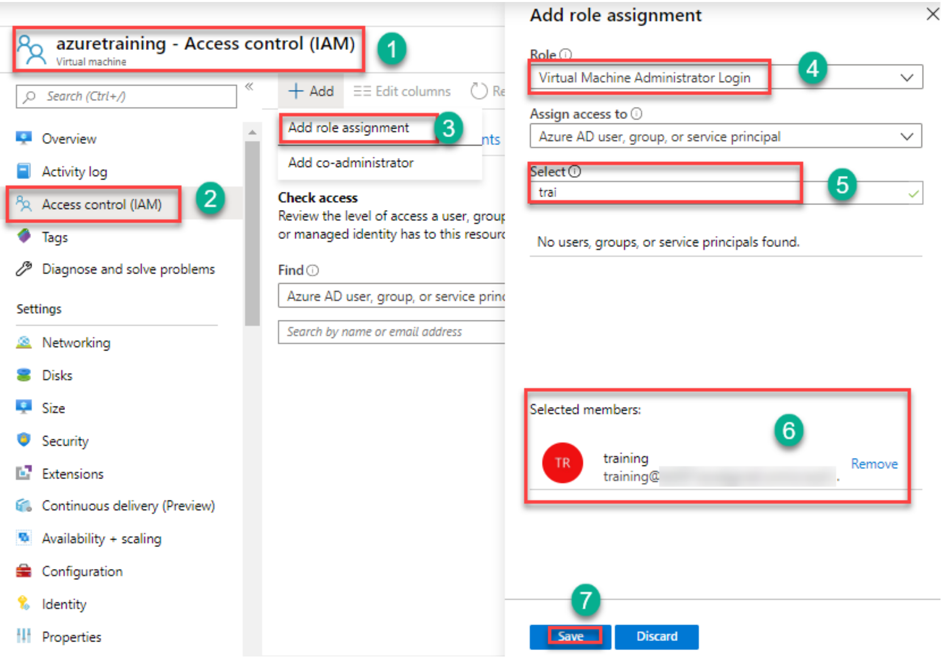
3. When you click on **Add role assignment**, select the role you want to assign the resources to:

1. Select the **Owner**, **Contributor**, or **Reader** role as per your requirements.

2. Type and search the user ID for which you want to provide the access.

3. Once you select all the required details, your screen will look like the following screenshot. Click on the **Save** button to apply the changes.

4. Once done, the user will be able to see the resources and access the resources.



Add role assignment

Role: Virtual Machine Administrator Login

Assign access to: Azure AD user, group, or service principal

Select: trai

No users, groups, or service principals found.

Selected members:

training
training@[redacted]

3- Custom RBAC role

Custom roles come in the picture when the built-in roles do not meet your customer or organization requirements. In that case, you can create a custom role using PowerShell, **Azure Resource Manager (ARM)** template, CLI, or REST API.

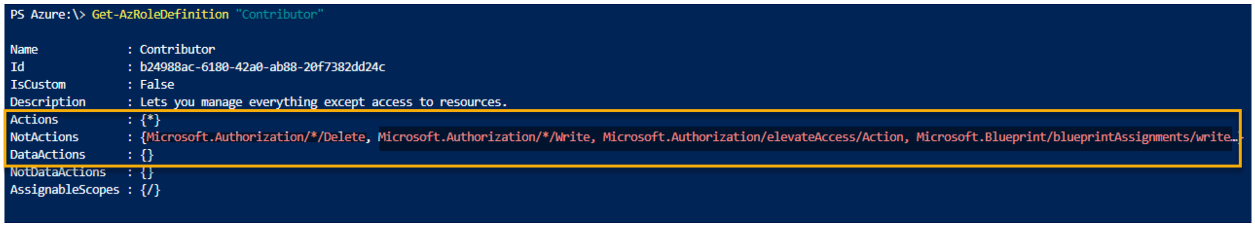
You can create up to 5000 custom roles in each tenant-level, but for a government cloud like, China, Germany, and so on, you can only create up to 2000 custom roles per tenant.

3.1- Creating the custom role

In this section, I will explain how to create the RBAC custom role and how to use existing built-in rules to create a new custom role.

If you want to allow any action to users, it should be listed in the Actions section and the deny user action can be put in the NotActions section while creating the custom RBAC.

If you would like to see what permission is available in the Azure contributor role, take a look at the following screenshot for the definition of the contributor role for more details:

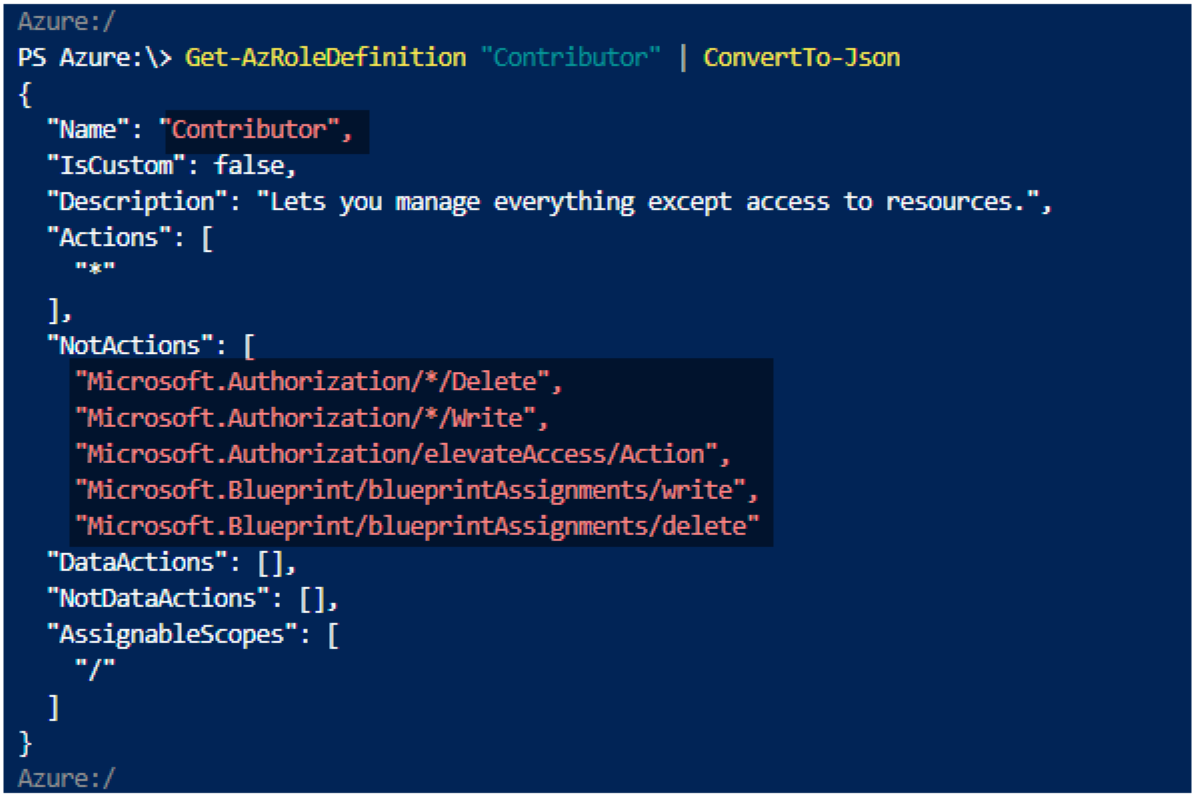


```
PS Azure:\> Get-AzRoleDefinition "Contributor"

Name             : Contributor
Id               : b24988ac-6180-42a0-ab88-20f7382dd24c
IsCustom         : False
Description      : Lets you manage everything except access to resources.
Actions          : {*}
NotActions       : {Microsoft.Authorization/*/Delete, Microsoft.Authorization/*/Write, Microsoft.Authorization/elevateAccess/Action, Microsoft.Blueprint/blueprintAssignments/write…
DataActions      : {}
NotDataActions   : {}
AssignableScopes : {/}
```

1. Please run the following command in PowerShell:

Get-AzRoleDefinition “Contributor” | ConvertTo-Json



```
Azure:/
PS Azure:\> Get-AzRoleDefinition "Contributor" | ConvertTo-Json
{
  "Name": "Contributor",
  "IsCustom": false,
  "Description": "Lets you manage everything except access to resources.",
  "Actions": [
    "*"
  ],
  "NotActions": [
    "Microsoft.Authorization/*/Delete",
    "Microsoft.Authorization/*/Write",
    "Microsoft.Authorization/elevateAccess/Action",
    "Microsoft.Blueprint/blueprintAssignments/write",
    "Microsoft.Blueprint/blueprintAssignments/delete"
  "DataActions": [],
  "NotDataActions": [],
  "AssignableScopes": [
    "/"
  ]
}
Azure:/
```

Once you get the output, copy the file and change the action or not action rule accordingly.

I will change the NotActions rule to Actions and create a custom role.

Save the file in the **JSON** format:

```
{
  "Name": "BPB_Contributor",
  "IsCustom": false,
   "Description": "Lets you manage everything except access to resources.",
  "Actions": [
     " Microsoft.Authorization/*/Delete",
    "Microsoft.Authorization/*/Write",
"Microsoft.Authorization/elevateAccess/Action",
"Microsoft.Blueprint/blueprintAssignments/write", "
  ],
  "NotActions": [
    "
"Microsoft.Blueprint/blueprintAssignments/delete"
  "DataActions": [],
  "NotDataActions": [],
  "AssignableScopes": [
    "/"
  ]
}
```

2. Go to PowerShell and connect to the subscription using the following command:

```
Connect-AzSubscription
```

3. Please provide the user ID and password to get authenticated. Then, run the following command to create a new role:

```
New-AzRoleDefinition -InputFile "C:\Temp\BPB_Role.json"
```

Once done, you will be able to create a custom role. It will look like the following screenshot, which I had created earlier: