

Manage access to Azure resources using RBAC

Use Case:

In this walkthrough task we will create some Azure resources that we can manage using Role-Based-Access-Control (RBAC), then we will view access control at subscription level, then view roles and permissions at resource group level for azure resources, and view individual user and all role assignments. You will then add a new role assignment for the virtual machine contributor role and then remove a role assignment for the resources you deployed.

Prerequisites:

You require need an Azure subscription to perform these steps. If you don't have one you can create one by following the steps outlined on the [Create your Azure free account today](#) webpage.

Steps:

Create Azure resources to manage

1. Sign into the Azure Portal and click on the **Cloud Shell** icon in the top right hand corner.
2. The **Cloud Shell** is launched in the bottom of the browser window.
3. Create a resource group into which we will place our resources by running the following Azure CLI command. You can copy and paste the command from the below directly into the Cloud Shell console, then press **Enter** to run the command. This command will run fine in either **powershell** **or** **bash** console.

```
``cli
az group create `
--name rbacrg `
--location westeurope
``
```

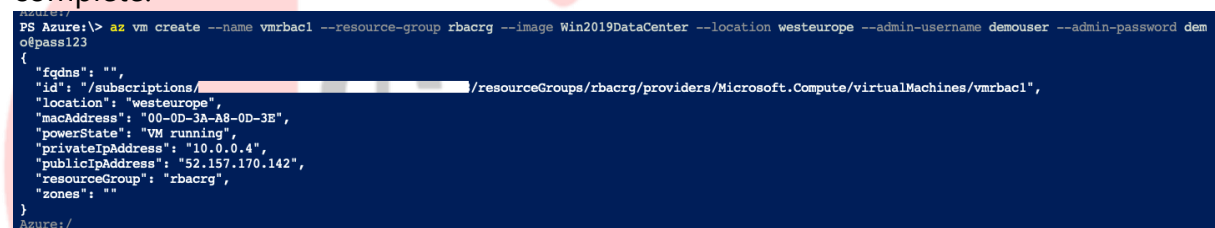
```
PS Azure:\> az group create --name rbacrg --location westeurope
{
  "id": "/subscriptions/[REDACTED]/resourceGroups/rbacrg",
  "location": "westeurope",
  "managedBy": null,
  "name": "rbacrg",
  "properties": {
    "provisioningState": "Succeeded"
  },
  "tags": null,
  "type": "Microsoft.Resources/resourceGroups"
}
```

4. Run the below Azure CLI command to create a virtual machine. Again, you can copy and paste the command from below directly into the Cloud Shell console and press **Enter** to run it.

```
cli

az vm create `
--name vmrbac1 `
--resource-group rbacrg `
--image Win2019Datacenter `
--location westeurope `
--admin-username azureuser `
--admin-password Password0134!
`
```

Note: The command will take 2 to 3 minutes to complete. The command will create a virtual machine and various resources associated with it such as storage, networking and security resources. You can close the Azure Cloud Shell once it is complete.



```
PS Azure:/> az vm create --name vmrbac1 --resource-group rbacrg --image Win2019Datacenter --location westeurope --admin-username demouser --admin-password dem
o@pass123
{
  "fqdns": "",
  "id": "/subscriptions/[redacted]/resourceGroups/rbacrg/providers/Microsoft.Compute/virtualMachines/vmrbac1",
  "location": "westeurope",
  "macAddress": "00-0D-3A-A8-0D-3E",
  "powerState": "VM running",
  "privateIpAddress": "10.0.0.4",
  "publicIpAddress": "52.157.170.142",
  "resourceGroup": "rbacrg",
  "zones": ""
}
```

View access control at subscription level

The next thing we need to do, in the context of access control, is to decide where to open the **Access control (IAM)** blade, through which we configure Role-Based-Access-Control (RBAC), and that depends on what resources you want to manage access for. i.e. do you want to manage access for everything in a management group, everything in a subscription, everything in a resource group, or a single resource? The **Access control (IAM)** blade is available at all of these levels and provides the same functionality in each. We will firstly have a look at the **Access control (IAM)** options for a subscription.

1. In the Azure portal, click **All services** and the **Subscriptions**, double click on a subscription from the subscriptions listed and then click on Access control (IAM) the scope.

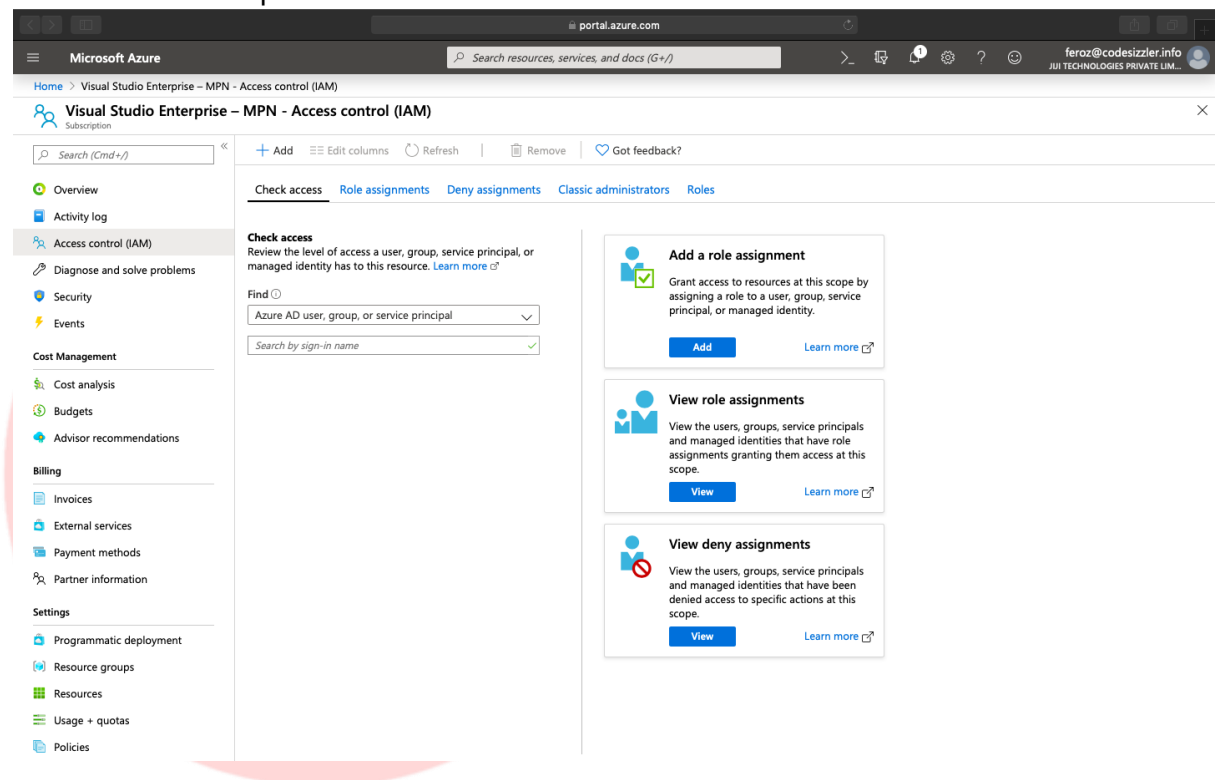
- **Note:** The screenshot above shows an example of the **Access control (IAM)** blade for a subscription. If you make any access control changes here, they would apply to the entire subscription. Likewise, any changes made at management group, resource group or individual resource level apply just at those levels.

View roles and permissions

A role definition is a collection of permissions that you use for role assignments. Azure has over 70 built-in roles for Azure resources. Follow these steps to view the available roles and permissions for the resources we deployed earlier.

1. Go to **Resource groups** and choose **rbacrg** i.e. the resource group you created earlier. Within the **rbacrg** resource group, click on **Access control (IAM)** and then select the **Roles** tab to see a list of all the built-in and custom roles.

Note: You can see the number of users and groups that are assigned to each role at the current scope.



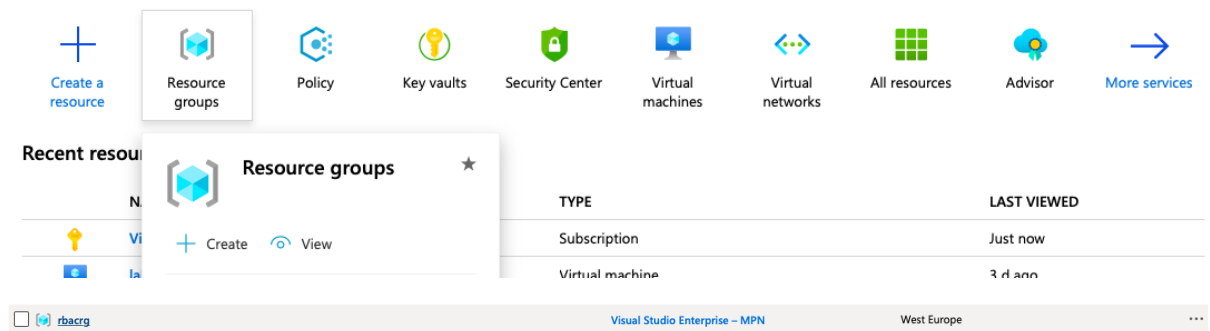
2. Click on the **Owner** role to see who has been assigned this role and also view the permissions for the role.

Note: As per the screenshot, there are two users listed who are assigned the Owner role. Your list of users will be different.

View individual user and all role assignments for a resource

When managing access, you want to know who has access, what are their permissions, and at what scope. To list access for a user, group, service principal, or managed identity, you view their role assignments.

1. In the resource group you created earlier i.e. **rbacrg** go to **Access control (IAM)** and select the **Check Access** tab.



2. In the **Find** boxes enter the below values, to search the directory for for display names, email addresses, or object identifiers. The matching results are displayed below the **Find** boxes

- Azure AD user, group, or service principal
- < your own user name i.e. in this case we used eamonn Kelly

Note: Your results will be different and related to your own user account.

2. Click the matching result to open the < **name** > **assignments - scope** pane. On this pane, you can see the roles assigned to the selected user and the scope. If there are any deny assignments at this scope or inherited to this scope, they will be listed. We can see the user has the role of **Owner** assigned and can manage everything.

Name	Type	Users	Groups
<input type="checkbox"/> Owner	BuiltInRole	2	0
<input type="checkbox"/> Contributor	BuiltInRole	0	0
<input type="checkbox"/> Reader	BuiltInRole	0	0
<input type="checkbox"/> AcrDelete	BuiltInRole	0	0
<input type="checkbox"/> AcrImageSigner	BuiltInRole	0	0
<input type="checkbox"/> AcrPull	BuiltInRole	0	0
<input type="checkbox"/> AcrPush	BuiltInRole	0	0
<input type="checkbox"/> AcrQuarantineReader	BuiltInRole	0	0
<input type="checkbox"/> AcrQuarantineWriter	BuiltInRole	0	0
<input type="checkbox"/> API Management Service Contributor	BuiltInRole	0	0
<input type="checkbox"/> API Management Service Operator Role	BuiltInRole	0	0
<input type="checkbox"/> API Management Service Reader Role	BuiltInRole	0	0
<input type="checkbox"/> App Configuration Data Owner	BuiltInRole	0	0
<input type="checkbox"/> App Configuration Data Reader	BuiltInRole	0	0
<input type="checkbox"/> Application Insights Component Contributor	BuiltInRole	0	0

4. Still on the resource group **Access control (IAM)** pane, click the **Role assignments** tab to view all the role assignments at this scope. On the **Role assignments** tab, you can see who has access at this scope.

Note: Some of roles present, are listed as **(Inherited)**. This means they are assigned from another scope. Access, in general, is either assigned specifically to this resource, or inherited from an assignment to the parent scope. Your values will be different to those displayed here.

Check access Role assignments Deny assignments Classic administrators Roles

Manage access to Azure resources for users, groups, service principals and managed identities at this scope by creating role assignments. [Learn more](#)

Name Type Role Scope Group by

Search by name or email All Owner All scopes Role

2 items (2 Users)

Name	Type	Role	Scope
Owner			
<input type="checkbox"/> AR Abdul Rasheed Feroz Khan (Guest) feroz@codesizzler.info	User	Owner	Subscription (Inherited)
<input type="checkbox"/> SC Suneetha Chowdary (Guest) suneetha@codesizzler.info	User	Owner	Subscription (Inherited)

Add a role assignment

In RBAC, to grant access, you assign a **Role** to a user, group, service principal, or managed identity. We will assign the role to a user in the following steps.

1. Open the resource group **Access control (IAM)** and click the **Role assignments** tab, then click **Add** and choose **Add role assignment** to open the **Add role assignment** pane.

Note: If you don't have permissions to assign roles, the **Add role assignment** option will be disabled.

Search (Cmd+/) << + Add Edit columns Refresh Remove Got feedback?

Check access **Add** Role assignments Deny assignments Classic administrators Roles

Manage access to Azure resources for users, groups, service principals and managed identities at this scope by creating role assignments. [Learn more](#)

Overview Activity log Access control (IAM)

+ Add Edit columns

Add role assignment

Add co-admin Add role assignment

Manage access to Azure resources for

2. In the **Add role assignment** pane fill in the following values, then click **Save** to assign the role.

- **Role:** select a Role from the drop down list i.e. *Virtual Machine Contributor*
- **Assign access to:** Azure AD user, group, or service principal
- **Select:** < type your own user name, and your user name should appear in the list, then click on a user name to select it >

Add role assignment
×

Role ⓘ
Virtual Machine Contributor

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

You are a guest user in this directory. You can search for users by their exact sign-in name, but you cannot search for groups or applications, and you cannot browse. ⓘ

imthiyas@codesizzler.info
✓

No users, groups, or service principals found.

MI

Mohammed Imthiyas (Guest)
imthiyas@codesizzler.info

Remove

Save

Discard

3. The user is now assigned the specified role at the selected scope.