



Azure 103 Module 6

Hands On - 2

Azure Certification Training

support@intellipaat.com

+91-7022374614

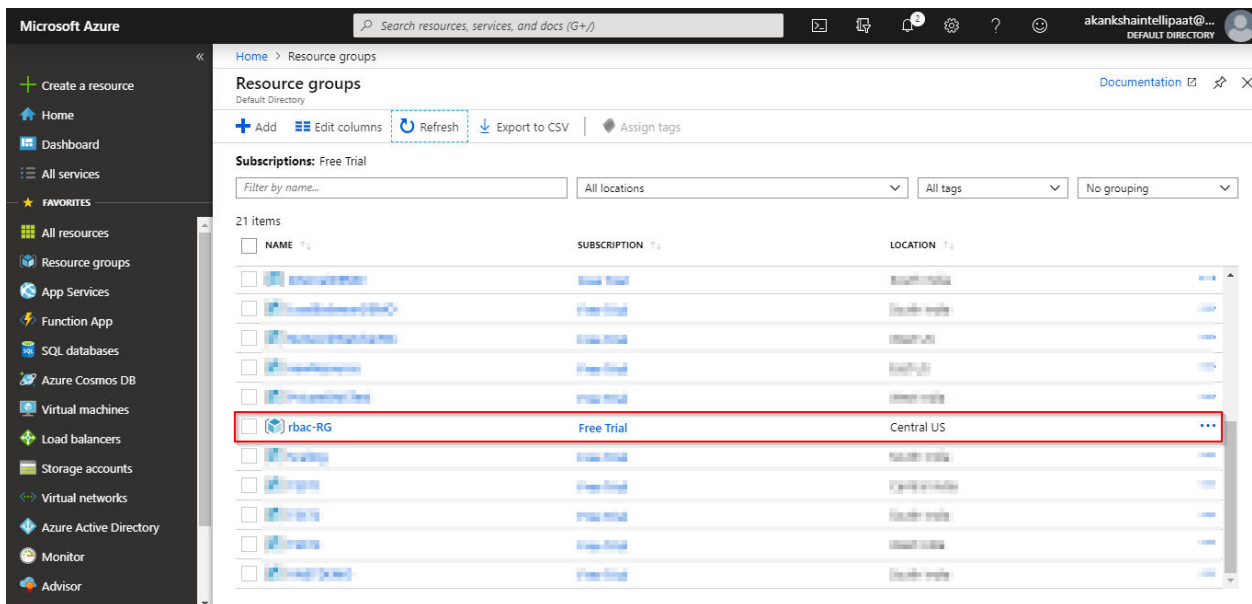
US: 1-800-216-8930(Toll Free)

Azure 103, Module 6, Hands On - 2

Problem Statement: Assign a role to configure access to Azure resources.

Solution:

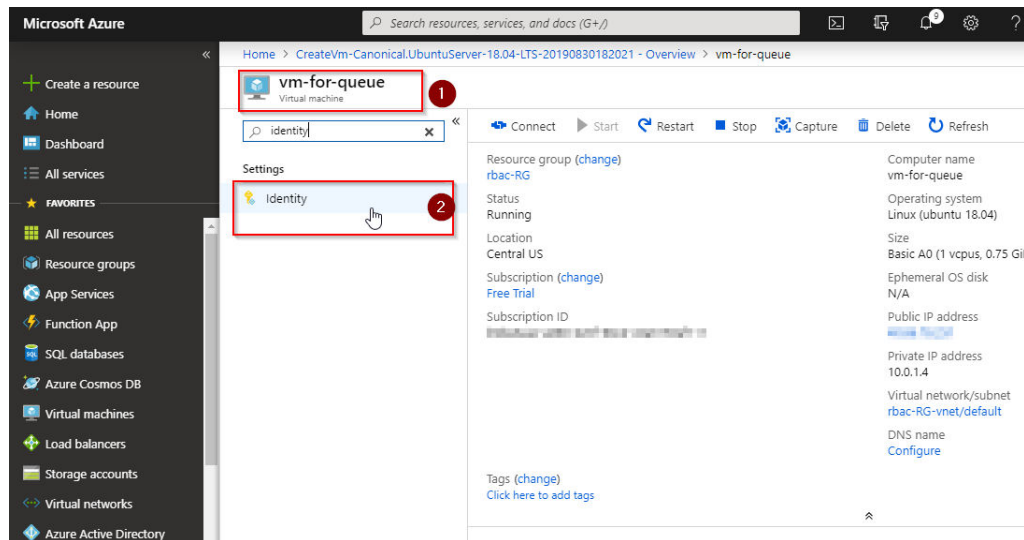
Step 1: Sign into the [Azure portal](#) and create a resource group named rbac-RG. We will use this resource group as a scope for this role assignment.



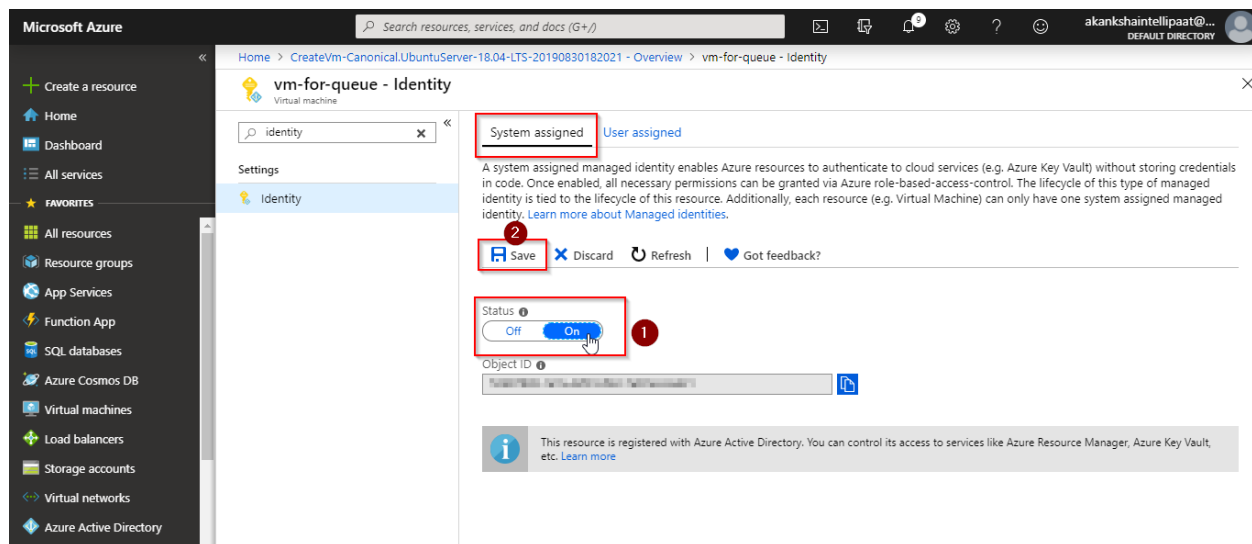
The screenshot shows the Microsoft Azure portal interface. The left sidebar contains navigation options like 'Create a resource', 'Home', 'Dashboard', 'All services', and 'FAVORITES'. The main content area is titled 'Resource groups' and shows a list of 21 items. The 'rbac-RG' resource group is highlighted with a red box. The table below shows the details of the resource groups.

NAME	SUBSCRIPTION	LOCATION
rbac-RG	Free Trial	Central US

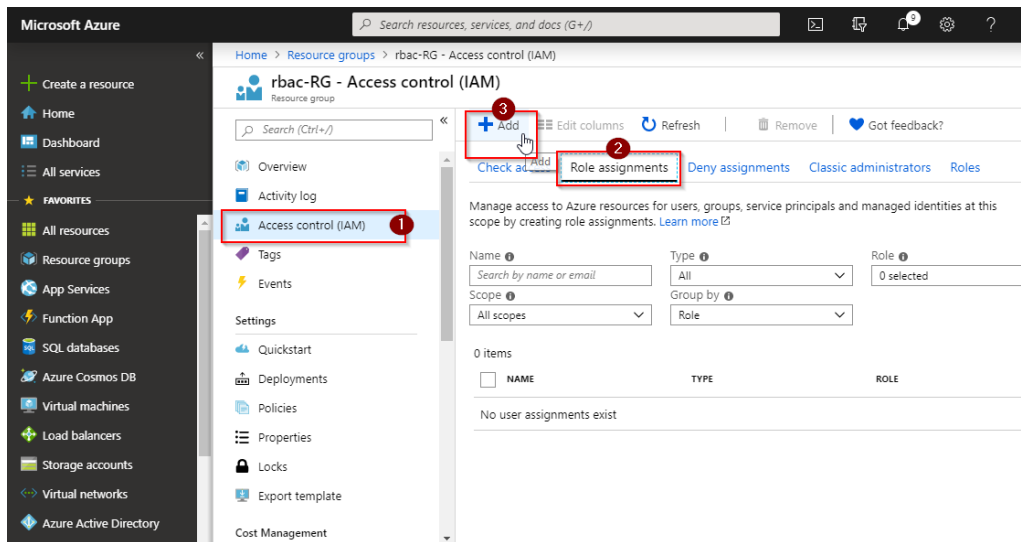
Step 2: Launch a basic virtual machine inside this resource group. After it is launched, go to the VM and select identity option from the left side panel.



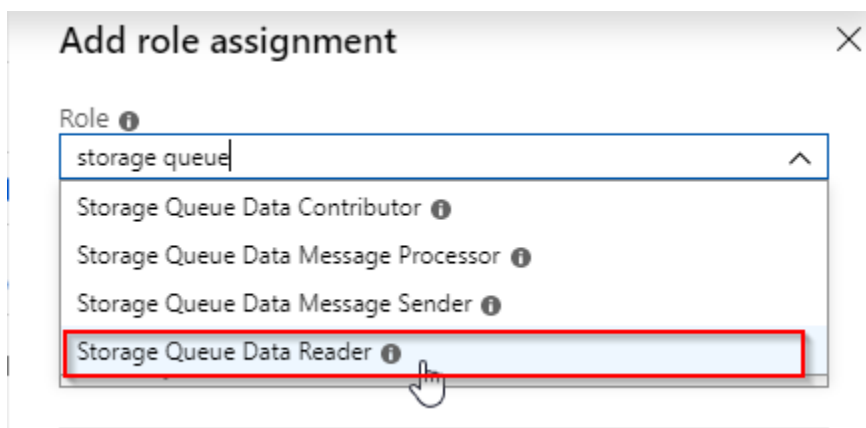
Step 3: In system assigned tab, switch the managed identity option to **on from off** and click on save.



Step 4: Go to your resource group and select Access control (IAM) option from the left side panel, then click on role assignment tab then click on add button. Select **“Add role assignment”** option from the drop down of add button



Step 5: In add role assignment blade that opens up, provide the relevant information. Select a role that you want to assign. For this demo, we will choose storage Queue Data Reader role.



Step 4: For **Assign access to** field, choose Virtual Machine.

Add role assignment ✕

Role ⓘ

Storage Queue Data Reader ▼

Assign access to ⓘ

Virtual Machine ^

Azure AD user, group, or service principal

User assigned managed identity

System assigned managed identity

App Service

Container Instance

Function App

Logic App

Virtual Machine

Virtual Machine Scale Set

Selected members:

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

Step 5: As soon as you are done with the previous step, the virtual machine for which you switched on the managed identity feature will get listed below the **select field**. Click on that VM to select it.

Add role assignment


Role ⓘ
Storage Queue Data Reader

Assign access to ⓘ
Virtual Machine

* Subscription
Free Trial

Select ⓘ

Search by name



vm-for-queue

subscriptions/vm-for-queue

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](#)

Save

Discard

Step 6: Click on save to save his role assignment.

Add role assignment ✕

Role ⓘ
Storage Queue Data Reader ▼


Assign access to ⓘ
Virtual Machine ▼

* Subscription
Free Trial ▼

Select ⓘ

No results to display.

Selected members:

 vm-for-queue Remove

Save

Discard

The role assignment will be created and you will be able to see as shown in the following screenshot.

Microsoft Azure

Search resources, services, and docs (G+)

Home > Resource groups > rbac-RG - Access control (IAM)

rbac-RG - Access control (IAM)

Resource group

Search (Ctrl+J)

+ Add Edit columns Refresh Remove Got feedback?

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

Search by name or email All Storage Queue Data Reader

Scope Group by

All scopes Role

1 items (1 Virtual Machines)

NAME	TYPE	ROLE
vm-for-queue	Virtual Machine	Storage Queue Data Reader

STORAGE QUEUE DATA READER