

Virtual Machine RBAC Roles

In this process, you're configuring role-based access control (RBAC) for a Windows Virtual Machine (VM) in Azure. The end goal is to manage user access to the VM effectively, ensuring secure connections and proper authentication protocols. By assigning RBAC roles and configuring user accounts, you control who can access and manage the VM, enhancing security and compliance within your Azure environment.

1. In your Azure portal go to Virtual Machine and create a Windows VM.
2. Now choose your resource group then give your VM a name then choose your region then choose your image as shown below.

Instance details

Virtual machine name *	windowsVM
Region *	(Europe) North Europe
Availability options	No infrastructure redundancy required
Security type	Standard
Image *	Windows Server 2022 Datacenter - x64 Gen2
See all images Configure VM generation	
 This image is compatible with additional security features. Click here to swap to the Trusted launch security type.	
VM architecture	<input type="radio"/> Arm64 <input checked="" type="radio"/> x64

3. After that choose a size of your choice then in the administrator account give it a username and password.

Size *	Standard_D2s_v3 - 2 vcpus, 8 GiB memory (₹12,085.69/month)
See all sizes	
Enable Hibernation (preview)	<input type="checkbox"/> <small>Hibernate is not supported by the size that you have selected. Choose a size that is compatible with Hibernate to enable this feature. Learn more</small>

Administrator account

Username *	demouser
Password *	*****
Confirm password *	*****

4. After that move to management, you will see this Microsoft Entra ID. You need to enable this option.

Microsoft Entra ID

Login with Microsoft Entra ID ⓘ



ⓘ RBAC role assignment of Virtual Machine Administrator Login or Virtual Machine User Login is required when using Microsoft Entra ID login. [Learn more](#) ⓘ

5. Then just move to review page and create your VM.
6. Now navigate to Microsoft Entra ID and create a new user.

Home > Default Directory | Users >

The screenshot shows the Microsoft Entra ID 'Users' page. On the left, there's a sidebar with links like 'All users', 'Audit logs', 'Sign-in logs', 'Diagnose and solve problems', 'Manage', and 'Troubleshooting + Support'. The main area has a search bar and a toolbar with 'New user', 'Download users', 'Bulk operations', 'Refresh', and 'Manage'. A dropdown menu is open under 'New user' with two options: 'Create new user' (selected) and 'Invite external user'. Below the menu, a table lists two users: 'demouser1' and 'PULKIT KUMAR'. The table has columns for 'User principal name' and 'User type'.

User principal name	User type
demouser1@pulkitkumar...	Member
pulkitkumar2711_gmail.c...	Member

7. Now give it a name then give the password and create your user.

Create new user ...

Create a new internal user in your organization

Basics Properties Assignments Review + create

Create a new user in your organization. This user will have a user name like alice@contoso.com. [Learn more](#)

Identity

User principal name * @ 

Domain not listed? [Learn more](#)

Mail nickname *

vmuser

Derive from user principal name

Display name *

vmuser

Password *

Password@1234



The new password must not be weak or commonly used.

Auto-generate password

Account enabled 



8. Once our user is in place then we need to login with it and change the password.

9. From here you need to copy the user principal name.

 Edit properties  Delete  Refresh |  Reset password  Revoke sessions  Manage view |  Got feedback?

Overview Monitoring Properties

Basic info



vmuser

vmuser@pulkitkumar2711gmail.onmicrosoft.com
Member

User principal name

vmuser@pulkitkumar2711gmail.onmicrosoft.com



Group memberships 0

Object ID

088112e6-fa4c-4fb6-ba92-dd61f549057d



Applications 0

Created date time

4 May 2024, 10:35 pm

Assigned roles 0

User type

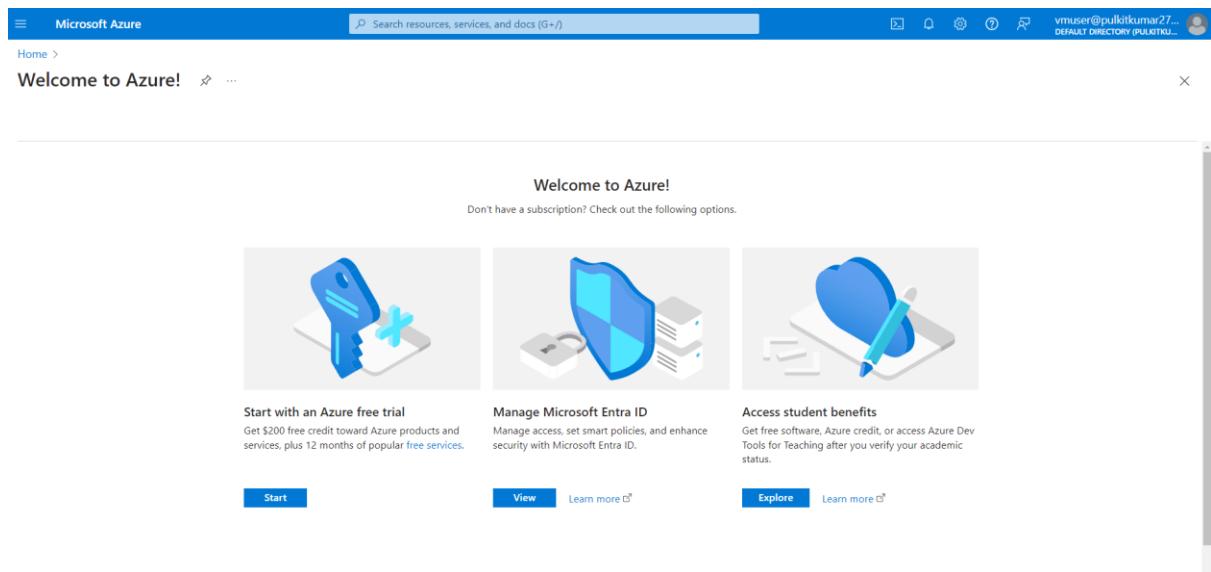
Member

Assigned licenses 0

Identities

pulkitkumar2711gmail.onmicrosoft.com

10. Once you have set up your user.



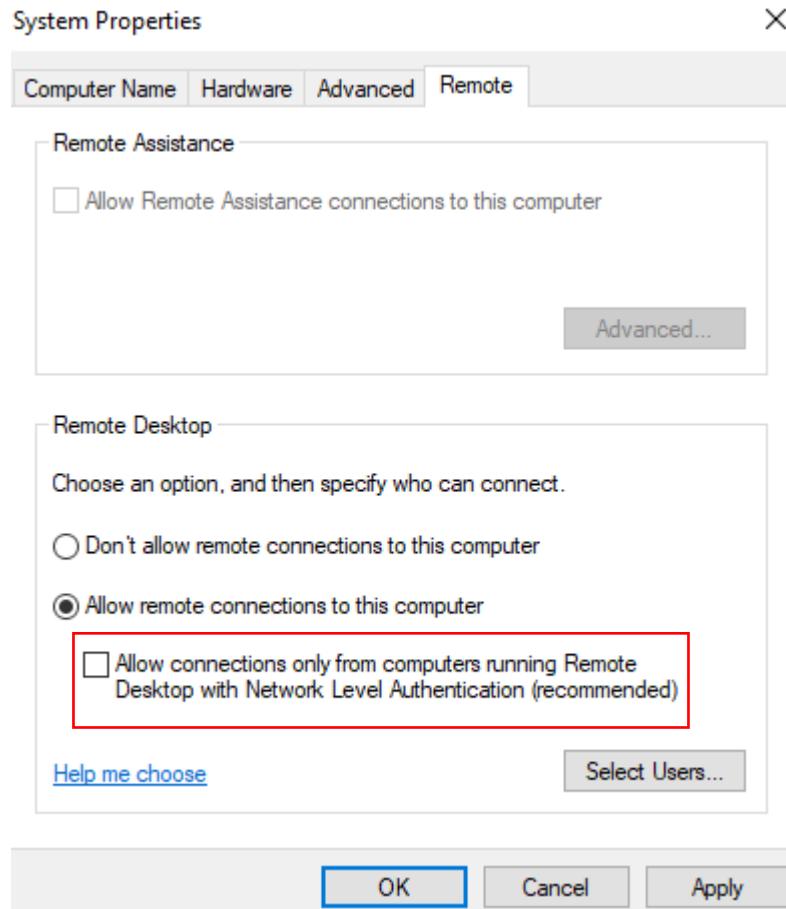
11. Then you are going to connect with your VM using your Azure admin account.
12. To do that you need to download the RDP file and then connect to it.
13. Inside your VM you need to choose the local server in your server manager and click on remote desktop.

A screenshot of the Microsoft Server Manager interface. The left sidebar shows navigation options: Dashboard, Local Server (which is selected and highlighted in blue), All Servers, and File and Storage Services. The main pane is titled "PROPERTIES" for "windowsVM". It displays various system settings:

Computer name	windowsVM
Workgroup	WORKGROUP
Microsoft Defender Firewall	Private: On
Remote management	Enabled
Remote Desktop	Enabled
NIC Teaming	Disabled
Ethernet 2	IPv4 address assigned by DHCP, IPv6 enabled
Azure Arc Management	Disabled
Operating system version	Microsoft Windows Server 2022 Datacenter
Hardware information	Microsoft Corporation Virtual Machine

The "Remote Desktop" row is highlighted with a red box.

14. Then in the system properties, you need to disable the highlighted option. Then click on apply and OK.
15. Then just close this session.



16. Then go to VM and go to IAM and choose to add role assignment.

The screenshot shows the 'Access control (IAM)' interface for a 'windowsVM' virtual machine. The top navigation bar includes a search bar, an 'Add' button, and a 'Download role assig' button. The left sidebar has 'Access control (IAM)' and 'Tags' options. A dropdown menu is open over the 'Add' button, showing 'Add role assignment' and 'Add co-administrator' options, with 'Add role assignment' highlighted by a red rectangle.

17. After that you need to choose the same role as shown below which is virtual machine user login.

Add role assignment ...

Role Members Conditions [Review + assign](#)

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Job function roles [Privileged administrator roles](#)

Grant access to Azure resources based on job function, such as the ability to create virtual machines.

virtual machine user login X Type : All Category : All

Name ↑	Description ↑	Type ↑↓	Category ↑↓	Details
Virtual Machine Data Access Administrator (prev...)	Manage access to Virtual Machines by adding or removing role assignments for the Virtual Machine Administrator Login an...	BuiltInRole	None	View
Virtual Machine User Login	View Virtual Machines in the portal and login as a regular user.	BuiltInRole	Compute	View

Showing 1 - 2 of 2 results.

18. This time choose your vmuser for member and then go to review page and assign this role.

Role **Members** Conditions [Review + assign](#)

Selected role Virtual Machine User Login

Assign access to User, group, or service principal Managed identity

Members [+ Select members](#)

Name	Object ID	Type
vmuser	088112e6-fa4c-4fb6-ba92-dd61f549057d	User

Description

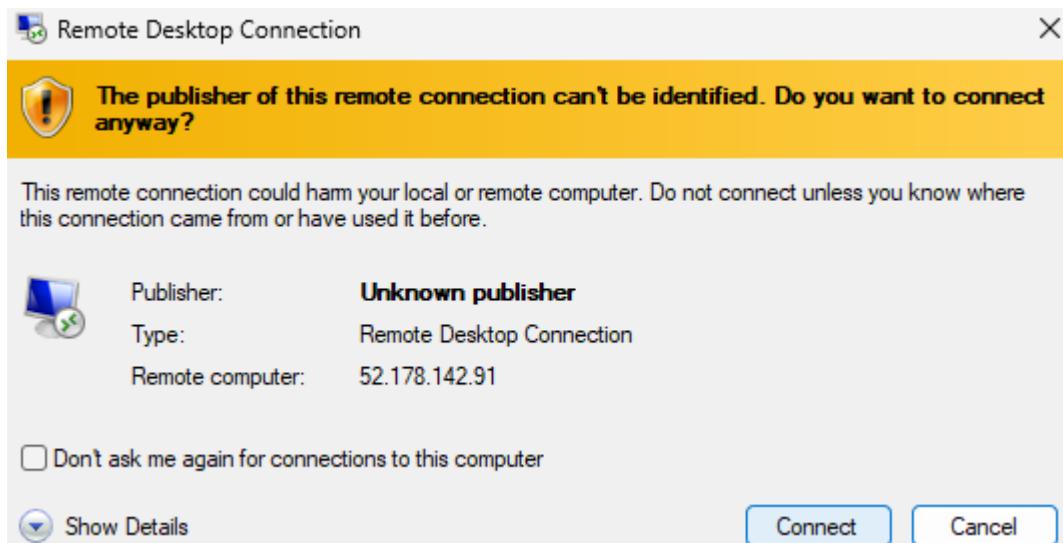
19. Now you need to go where you have stored the RDP file which was downloaded to login to your VM.

20. After that you need to right-click on it then choose open with Notepad. Then you have to add this data in your file. Just keep in mind the IP should be yours and the username should also be yours.

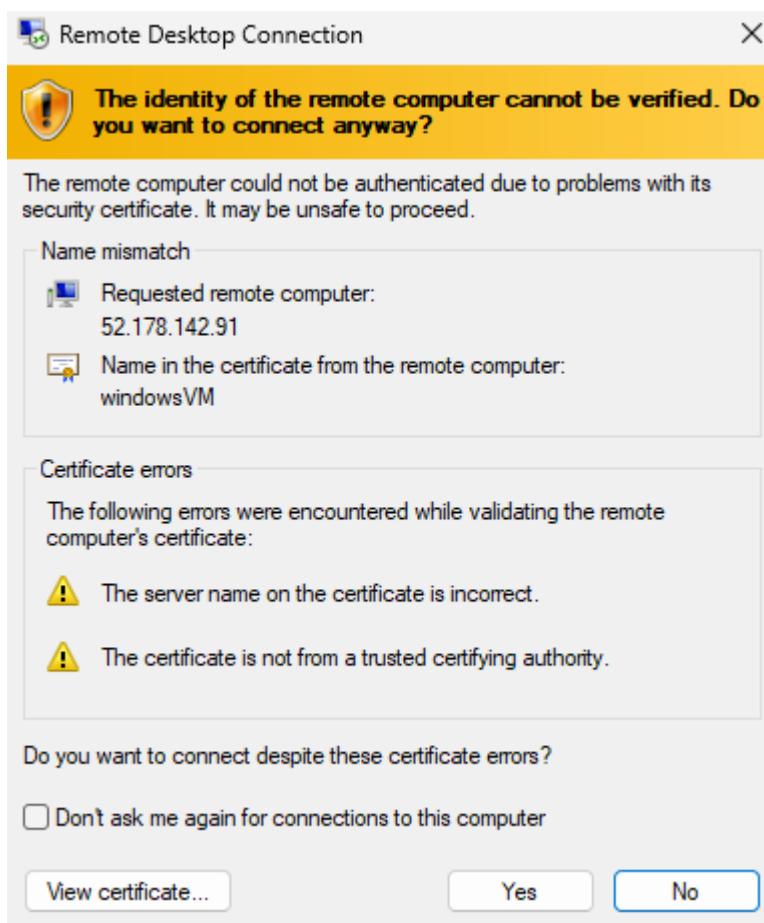
21. Then just save it.

```
full address:s:52.178.142.91:3389
prompt for credentials:i:0
domain:s:AzureAD
enablecredssp support:i:0
authentication level:i:2
username:s:\AzureAD\vmuser@pulkitkumar2711gmail.onmicrosoft.com
```

22. After that double click on the file to open. It will ask you to connect.

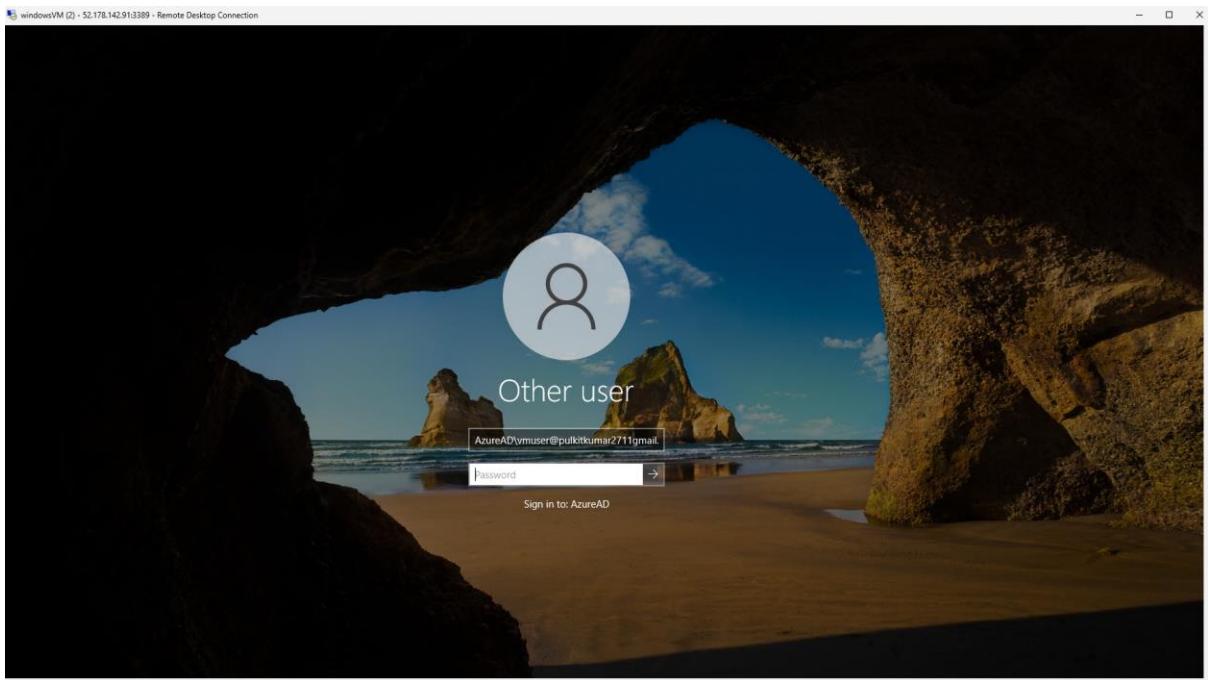


23. Then you will get this verification message just click on yes.



24. Below you can see that it is asking you to log in as VM user.

25. Just enter your password and login as VM user.



26. Once you are done with the lab delete your resources.