

APEX Institute of Technology Information Security

Experiment – 2

Student Name: Hemant Sharma

Branch: Information Security

Semester: 5th

Subject Name: Network Security essentials Lab

UID: 20BCS3600

Section/Group: 20BIS1 B

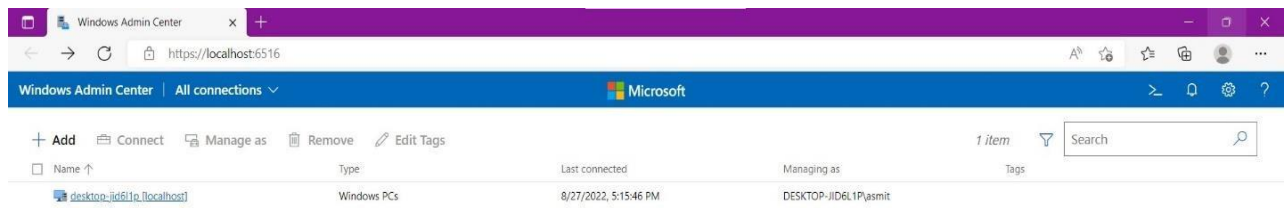
Date: 27/08/2022

Subject Code: 20CSB-332

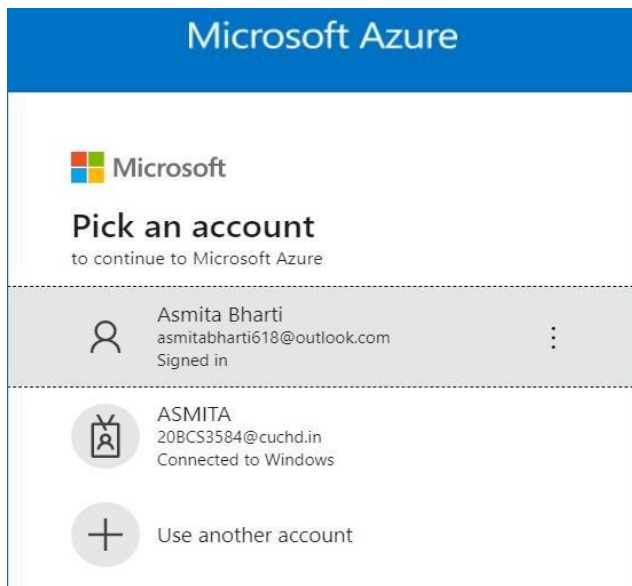
Aim: Implementing role-based access control in windows

Steps for Role-Based Access control.

1. Open Window Admin Centre



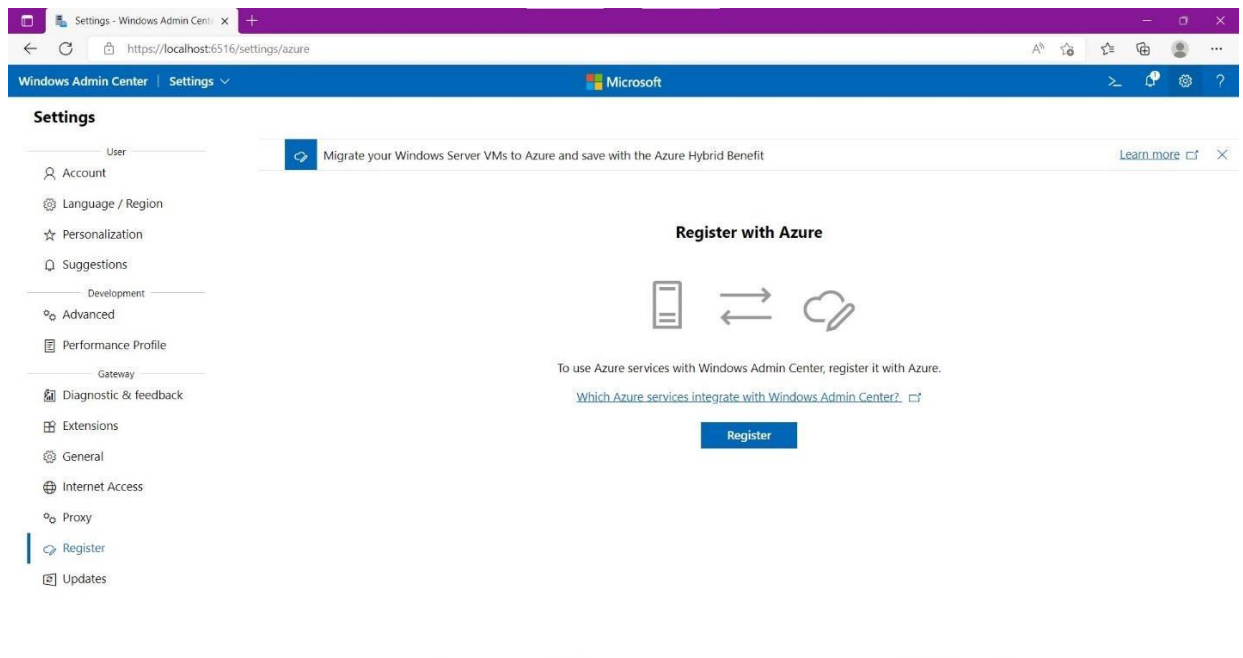
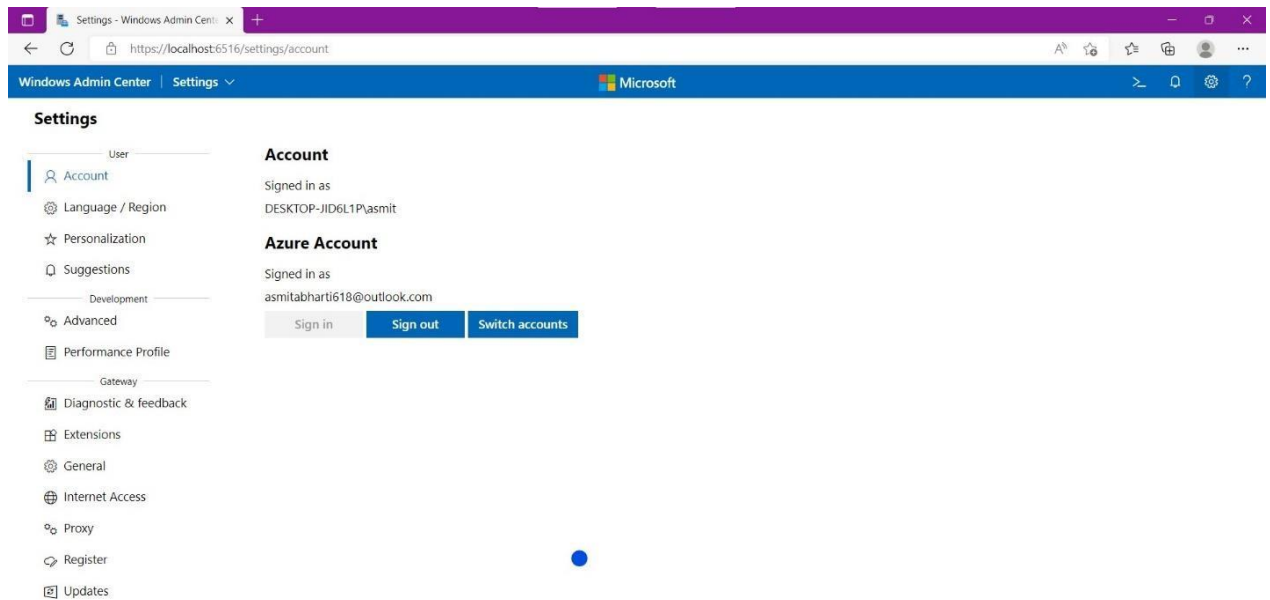
2. For connecting Window Admin centre with Microsoft Azure, we must create a Microsoft account



APEX Institute of Technology

Information Security

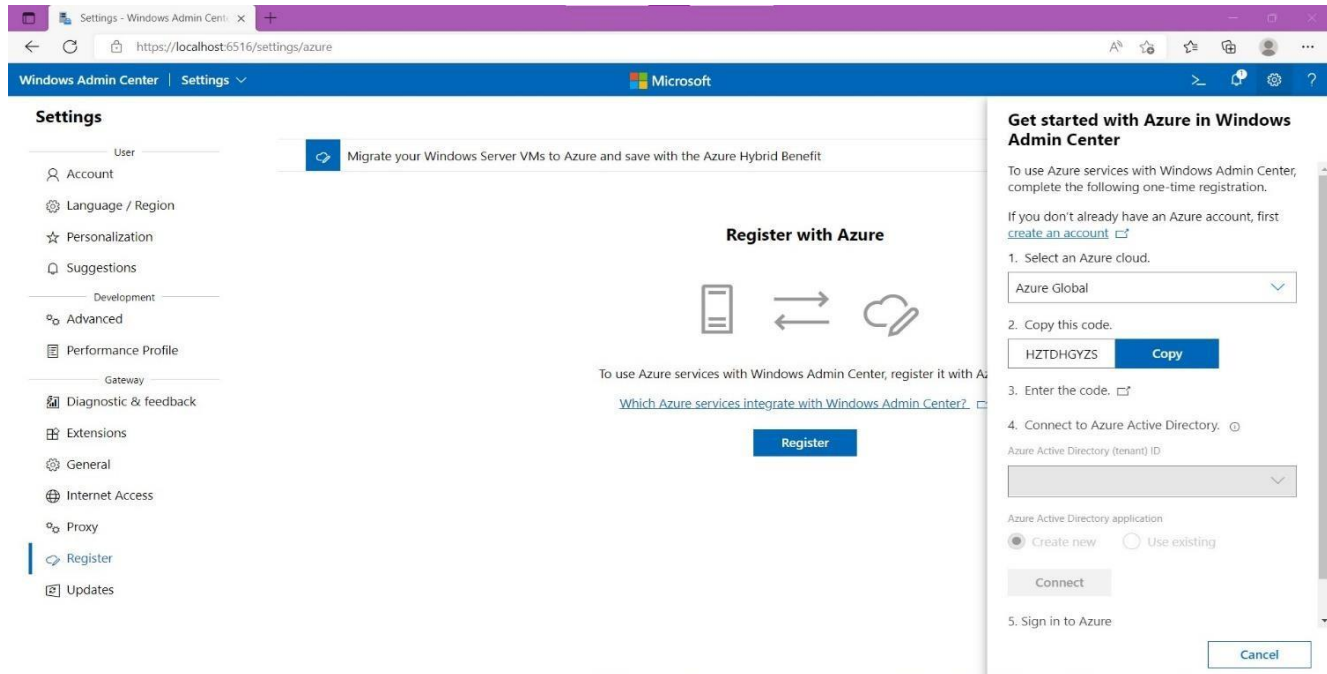
3. Now Go to settings and in settings click on **Register** and then register in Azure



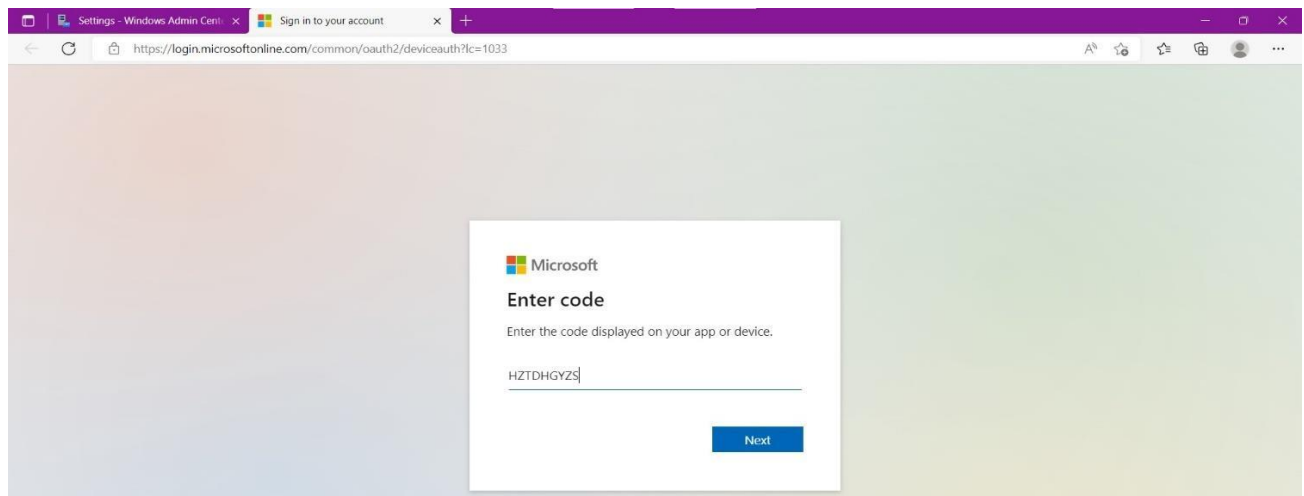
APEX Institute of Technology

Information Security

4. After Clicking on register a pop-up window will appear named **“Get started with Azure in Windows admin centre”** will appear.



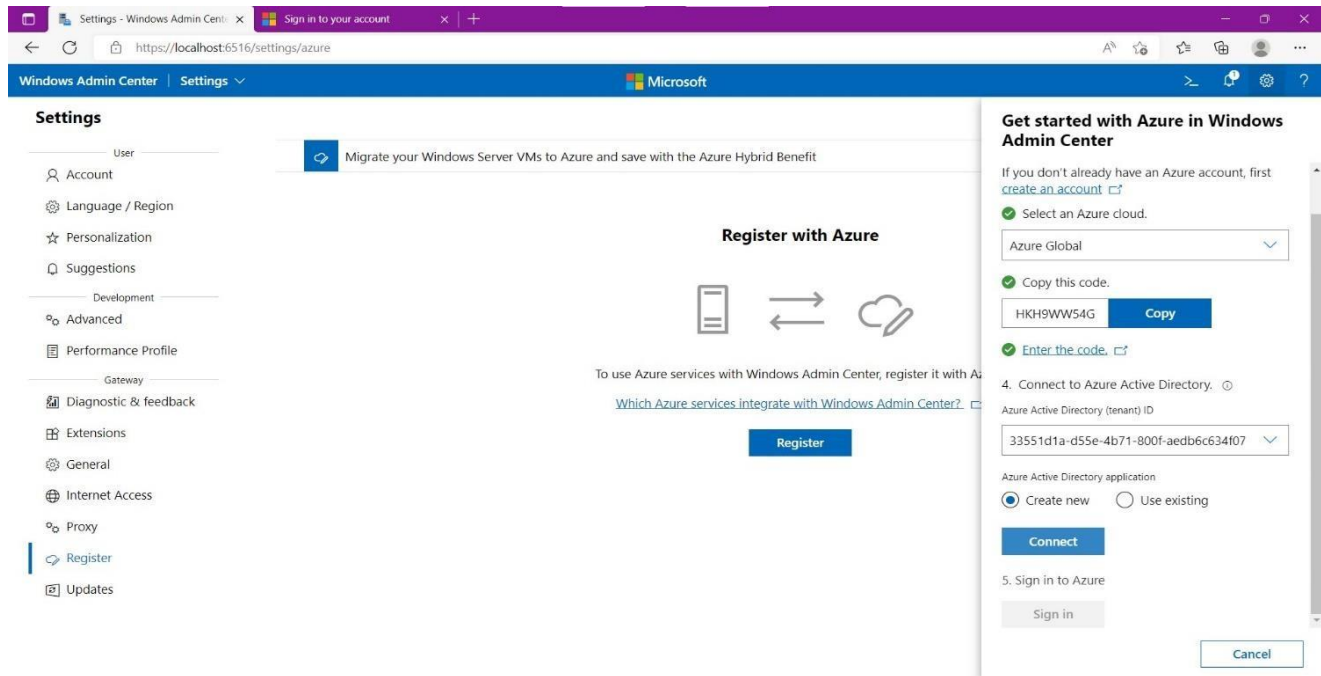
5. In the pop-up window copy the code and click on **“Enter the code”** a new window will appear and now paste the code.



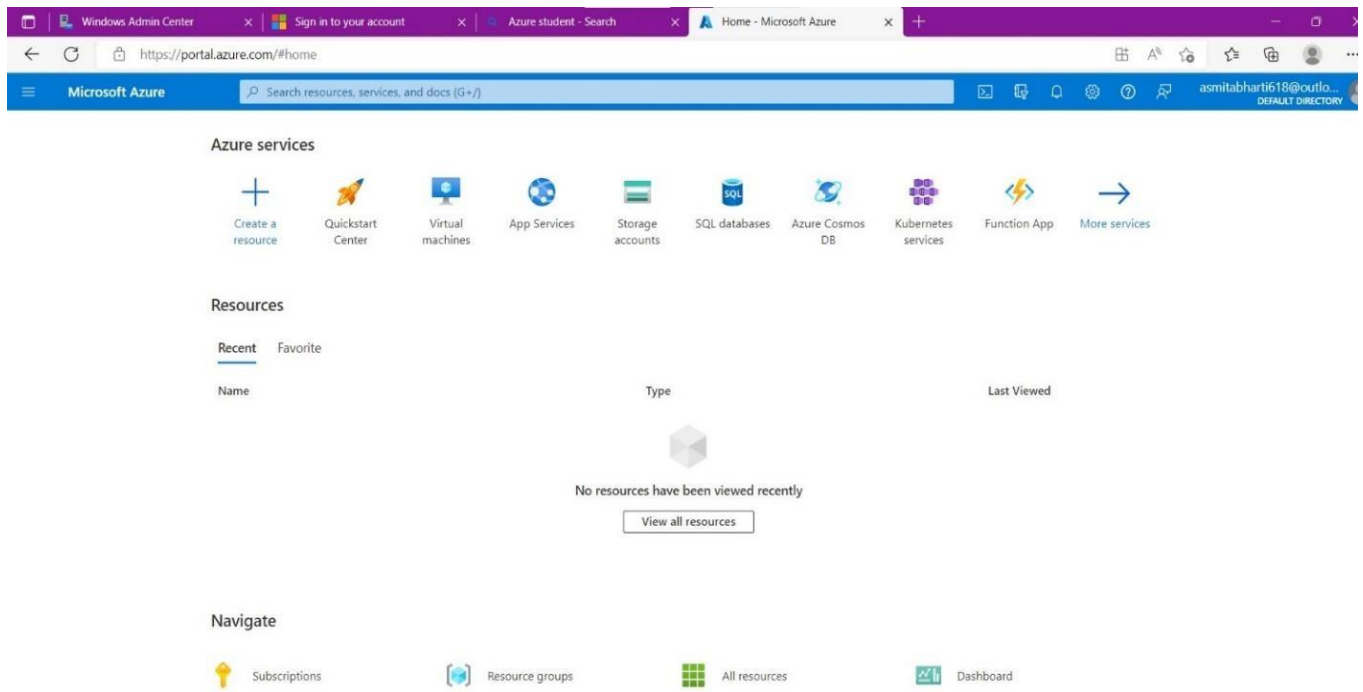
APEX Institute of Technology

Information Security

6. Under Azure Active Directory application, select **“Create new”** and click on Connect.



7. Now, you will be redirected to Microsoft Azure.



APEX Institute of Technology

Information Security

8. In the search bar, search for Azure AD roles. Select Azure AD roles and administrators

The screenshot shows the Microsoft Azure portal interface. The search bar at the top contains the text 'Azure AD role'. Below the search bar, a dropdown menu displays various results categorized under 'Services', 'Resources', 'Resource Groups', 'Marketplace', and 'Documentation'. The 'Services' category is expanded, showing a list of Azure AD roles and administrators, including 'Azure AD roles and administrators', 'Create custom Azure AD roles', 'Azure AD Identity Protection', 'Azure AD Security', and 'Azure AD Risky workload identities'. The 'Resources' category is also visible, showing 'Azure Cosmos DB' and 'Azure Database for MySQL servers'. The 'Documentation' category is expanded, showing a list of documentation links related to Azure AD roles and administrators.

9. After selecting Azure Ad roles and administrator we can see that our role is Global administrator. Now we can change the roles of users in it.

The screenshot shows the Microsoft Azure portal interface, specifically the 'All roles' page for Azure Active Directory. The page displays a list of roles and their descriptions. The 'Your Role' is identified as 'Global administrator'. Below the list, there is a section for 'Administrative roles' with a description: 'Administrative roles are used for granting access to privileged actions in Azure AD. We recommend using these built-in roles for delegating access to manage broad application configuration permissions without granting access to manage other parts of Azure AD not related to application configuration. Learn more.' The list of roles includes:

Role	Description	Type
Application administrator	Can create and manage all aspects of app registrations and enterprise apps.	Built-in
Application developer	Can create application registrations independent of the 'Users can register applications' setting.	Built-in
Attack payload author	Can create attack payloads that an administrator can initiate later.	Built-in
Attack simulation administrator	Can create and manage all aspects of attack simulation campaigns.	Built-in
Attribute assignment administrator	Assign custom security attribute keys and values to supported Azure AD objects.	Built-in
Attribute assignment reader	Read custom security attribute keys and values for supported Azure AD objects.	Built-in
Attribute definition administrator	Define and manage the definition of custom security attributes.	Built-in
Attribute definition reader	Read the definition of custom security attributes.	Built-in
Authentication administrator	Has access to view, set, and reset authentication method information for any non-admin user.	Built-in
Authentication policy administrator	Can create and manage all aspects of authentication methods and password protection policies.	Built-in

APEX Institute of Technology

Information Security

10. Click on your roles.

The screenshot shows the Microsoft Azure portal interface. The user is logged in as 'Asmita Bharti'. The left sidebar contains navigation options: 'Diagnose and solve problems', 'Manage' (with sub-items: Profile, Assigned roles, Administrative units, Groups, Applications, Licenses, Devices, Azure role assignments, Authentication methods), and 'Activity' (with sub-items: Sign-in logs, Audit logs). The 'Assigned roles' section is selected. The main content area shows 'Administrative roles' with a search bar and a table of assigned roles. The table has columns: Role, Description, Resource Name, Resource Type, Assignment Path, and Type. One role is listed: 'Global administrator' with a description 'Can manage all aspects of Azure AD and Microsoft services that...'. The 'Resource Name' is 'Directory', 'Resource Type' is 'Organization', 'Assignment Path' is 'Direct', and 'Type' is 'Built-in'.

11. Click on Add assignments. A pop up will appear named Directory roles search user in it.

The screenshot shows the Microsoft Azure portal with the 'Directory roles' search pop-up open. The pop-up has a title bar 'Directory roles' and a close button. It contains a 'Sort' dropdown, a message 'To assign custom roles to a user, your organization needs Azure AD Premium P1 or P2.', and a section 'Choose admin roles that you want to assign to this user. Learn more'. Below this is a search bar with 'User' entered and an 'Add filters' button. A list of roles is displayed, each with a checkbox, a role name, and a description. The roles are: 'Application developer', 'Authentication administrator', 'Azure AD joined device local administrator', 'Directory writers', 'External ID user flow administrator', 'External ID user flow attribute administrator', 'Guest inviter', 'Office apps administrator', and 'Privileged authentication administrator'. An 'Add' button is at the bottom of the list.

APEX Institute of Technology

Information Security

12. Now we can assign any role to the user. Select any role you want to assign to the user. Click on Add. (Here, we are selecting Directory writers).

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation pane includes sections like 'Manage' (Profile, Assigned roles, Administrative units, Groups, Applications, Licenses, Devices, Azure role assignments, Authentication methods) and 'Activity' (Sign-in logs, Audit logs). The main content area is titled 'Asmita Bharti | Assigned roles'. A modal window titled 'Directory roles' is open, displaying a list of administrative roles. The 'Directory writers' role is selected with a blue checkmark. Below the list, an 'Add' button is visible.

Role	Description
<input type="checkbox"/> Global administrator	Can manage all aspects of Azure AD and other Microsoft services.
<input checked="" type="checkbox"/> Directory writers	Can read and write basic directory information. For granting access to applications, not intended for users.
<input type="checkbox"/> Application developer	Can create application registrations independent of the 'Users can register applications' setting.
<input type="checkbox"/> Authentication administrator	Has access to view, set, and reset authentication method information for any non-admin user.
<input type="checkbox"/> Azure AD joined device local administrator	Users assigned to this role are added to the local administrators group on Azure AD-joined devices.
<input type="checkbox"/> External ID user flow administrator	Can create and manage all aspects of user flows.
<input type="checkbox"/> External ID user flow attribute administrator	Can create and manage the attribute schema available to all user flows.
<input type="checkbox"/> Guest inviter	Can invite guest users independent of the 'members can invite guests' setting.
<input type="checkbox"/> Office apps administrator	Can manage Office apps cloud services, including policy and settings management, and manage the ability to select, unselect and publish "what's new" feature content to end-user's devices.
<input type="checkbox"/> Privileged authentication administrator	Allowed to view, set and reset authentication method information for

13. Now refresh the page. After refreshing we can see the Directory writer roles assigned to the user.

The screenshot shows the Microsoft Azure portal interface after refreshing. The 'Assigned roles' section now displays a table with the assigned roles for user Asmita Bharti.

Role	Description	Resource Name	Resource Type	Assignment Path	Type
<input type="checkbox"/> Directory writers	Can read and write basic directory information. For granting acc...	Directory	Organization	Direct	Built-in
<input type="checkbox"/> Global administrator	Can manage all aspects of Azure AD and Microsoft services that ...	Directory	Organization	Direct	Built-in