

Introduction to Cloud Computing

LAB 02a

Name: Muhammad Yahya

ID: 2280155

BS-SE 7B

Task 1: Implement Management Groups

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and a Copilot icon. The user's profile is visible in the top right corner, showing the email address bsse2280155@szabist.pk. The main content area is titled "Resource Manager | Management groups". The left sidebar contains a navigation menu with options like "Resource Manager", "All resources", "Favorite resources", "Recent resources", "Resource groups", "Tags", "Organization", "Service groups", "Management groups" (selected), "Subscriptions", "Tools", "Deployments", and "Help". The main pane displays the "Overview" tab for Management groups. It shows a table with one subscription, "Azure for Students", under the "Tenant Root Group". The table has columns for Name, Type, ID, and Total subscriptions.

Name	Type	ID	Total subscriptions
Tenant Root Group	Management group	d7e692a5-cccf-417c-b67f-0ded375904c4	1
Azure for Students	Subscription	db878fcc-8781-42d0-a61d-55de3d976446	

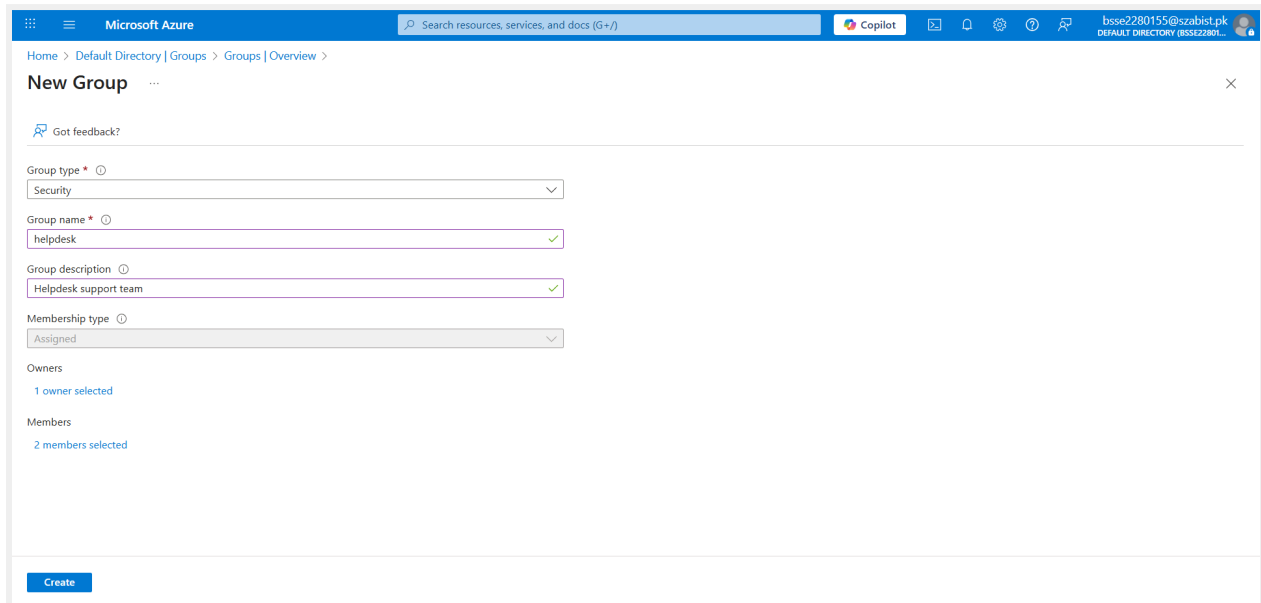
The screenshot shows the "Create management group" dialog box in the Microsoft Azure portal. The dialog box is titled "Create management group" and contains the following fields:

- Management group ID (Cannot be updated after creation): az104-mg1
- Management group display name: az104-mg1

The dialog box also includes a "Submit" button and a "Cancel" button.

Task 2: Review and assign a built-in Azure role

- **Note:** In the following steps, you will assign the role to the **helpdesk** group. If you do not have a Help Desk group, take a minute to create it.



Microsoft Azure

Home > Default Directory | Groups > Groups | Overview >

New Group

Got feedback?

Group type *

Group name *

Group description

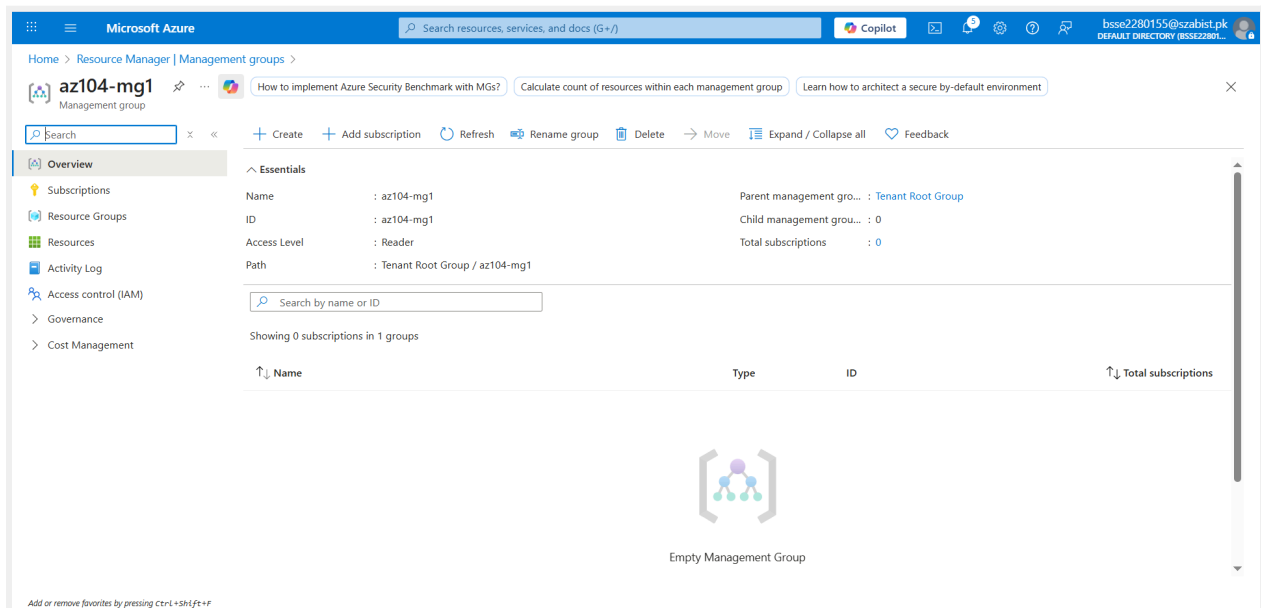
Membership type

Owners
1 owner selected

Members
2 members selected

Create

- Select the **az104-mg1** management group.



Microsoft Azure

Home > Resource Manager | Management groups >

az104-mg1

Management group

Search resources, services, and docs (G+)

How to implement Azure Security Benchmark with MGs? Calculate count of resources within each management group Learn how to architect a secure by-default environment

Search

+ Create + Add subscription Refresh Rename group Delete Move Expand / Collapse all Feedback

Overview

Subscriptions

Resource Groups

Resources

Activity Log

Access control (IAM)

Governance

Cost Management

Essentials

Name : az104-mg1

ID : az104-mg1

Access Level : Reader

Path : Tenant Root Group / az104-mg1

Parent management gro... : Tenant Root Group

Child management grou... : 0

Total subscriptions : 0

Search by name or ID

Showing 0 subscriptions in 1 groups

Name	Type	ID	Total subscriptions
------	------	----	---------------------

Empty Management Group

Add or remove favorites by pressing Ctrl+Shift+F

- Select the **Access control (IAM)** blade, and then the **Roles** tab.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and various utility icons. The breadcrumb trail indicates the path: Home > Resource Manager | Management groups > az104-mg1. The main header shows 'az104-mg1 | Access control (IAM)' with a close button. Below the header, there's a search bar and a set of tabs: 'Check access', 'Role assignments', 'Roles' (selected), and 'Deny assignments'. A warning banner at the top states: 'Action required: 1 user has elevated access in your tenant. You should take immediate action and remove all role assignments with elevated access. View role assignments'. Below the tabs, a description reads: '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'. There are three sub-tabs: 'All' (selected), 'Job function roles', and 'Privileged administrator roles'. A search bar is provided with the placeholder 'Search by role name, description, permission, or ID'. Below this is a table of built-in roles.

Name	Description	Type	Category	Details
Owner	Grants full access to manage all resources, including the ability to assign roles in Azur...	BuiltInRole	General	View
Contributor	Grants full access to manage all resources, but does not allow you to assign roles in A...	BuiltInRole	General	View
Reader	View all resources, but does not allow you to make any changes.	BuiltInRole	General	View
Access Review Operator Service ...	Lets you grant Access Review System app permissions to discover and revoke access ...	BuiltInRole	None	View
AcrDelete	acr delete	BuiltInRole	Containers	View
AcrImageSigner	Planned DEPRECATION on March 31, 2028. Grant the signing permission for content t...	BuiltInRole	Containers	View
AcrPull	acr pull	BuiltInRole	Containers	View
AcrPush	acr push	BuiltInRole	Containers	View

- Select **Add**, from the drop-down menu, select **Add role assignment**.

The screenshot shows the 'Add role assignment' wizard in the Microsoft Azure portal. The top navigation bar is the same as the previous screenshot. The breadcrumb trail is: Home >. The main header shows 'Add role assignment' with a close button. Below the header, there are four tabs: 'Role', 'Members', 'Conditions', and 'Review + assign' (selected). The 'Role' tab is active, showing the following details:

- Role:** Virtual Machine Contributor
- Scope:** /providers/Microsoft.Management/managementGroups/az104-mg1
- Members:** A table with columns 'Name', 'Object ID', and 'Type'. It contains one entry: 'helpdesk' with Object ID '377d0c9-e071-4941-8d94-40fc5a93a7ab' and Type 'Group'.
- Description:** No description
- Condition:** None

At the bottom of the wizard, there are three buttons: 'Review + assign' (highlighted in blue), 'Previous', and 'Next'. A 'Feedback' link is located in the bottom right corner.

- Continue on the **Access control (IAM)** blade.
- On the **Role assignments** tab, confirm the **helpdesk** group has the **Virtual Machine Contributor** role.

Microsoft Azure

Home > Resource Manager | Management groups > az104-mg1

az104-mg1 | Access control (IAM)

Search resources, services, and docs (G+J)

Search

Overview

Subscriptions

Resource Groups

Resources

Activity Log

Access control (IAM)

Governance

Cost Management

Action required: 1 user has elevated access in your tenant. You should take immediate action and remove all role assignments with elevated access. [View role assignments](#)

Check access **Role assignments** Roles Deny assignments

Search by name or email

Type: All Role: All Scope: All scopes Group by: Role

All (3) Job function roles (1) Privileged administrator roles (2)

Name	Type	Role	Scope	Condition
> Owner (1)				
> User Access Administrator (1)				
Virtual Machine Contributor (1)				
helpdesk 377dc0c9-e071-4941-8d94-4...	Group	Virtual Machine Contributor	This resource	Add

Showing 1 - 3 of 3 results.

Add or remove favorites by pressing Ctrl+Shift+F

Task 3: Create a custom RBAC role

- Navigate to the **Access control (IAM)** blade.
- Select **Add**, from the drop-down menu, select **Add custom role**.

Microsoft Azure

Home > Resource Manager | Management groups > az104-mg1 | Access control (IAM) >

Create a custom role

Basics Permissions Assignable scopes JSON Review + create

To create a custom role for Azure resources, fill out some basic information. [Learn more](#)

Custom role name *

Description

Baseline permissions ☒ Clone a role ☐ Start from scratch ☐ Start from JSON

Role to clone

[Review + create](#) [Previous](#) [Next](#) [Feedback](#)

- Select **Add**, from the drop-down menu, select **Add custom role**.

Microsoft Azure

Home > Resource Manager | Management groups > az104-mg1 | Access control (IAM) >

Create a custom role

Basics **Permissions** Assignable scopes JSON Review + create

[+ Add permissions](#) [+ Exclude permissions](#)

Click Add permissions to select the permissions you want to add to your custom role. To add a wildcard (*) permission, you must manually add the permission. To exclude specific permissions from a wildcard permission, click Exclude permissions.

Permission	Description
Microsoft.Authorization/*/read	Gets the permissions for the specified resource.
Microsoft.Resources/subscriptions/resourceGroups/read	Gets the permissions for the specified resource group.
Microsoft.Support/*	Gets the permissions for the specified resource.

[Add](#) [Cancel](#)

Microsoft.Support permissions

< All resource providers

Exclude permissions enable you to subtract specific permissions from a wildcard (*) permission. If your custom role has a permission with a wildcard (*) and you don't want to include all the permissions under the wildcard, search for permissions to subtract from the wildcard. For example, search for "virtual machines" to find permissions related to virtual machines.

☒ Not Actions ☐ Not Data Actions

Permission	Description
<input checked="" type="checkbox"/> Microsoft.Support	
<input checked="" type="checkbox"/> Other : Registers Support Resource Provider	Registers Support Resource Provider
<input type="checkbox"/> Other : Look Up Resource Id	Looks up resource id for resource type
<input type="checkbox"/> Other : Check Name Availability	Checks that name is valid and not in use for resource type
<input type="checkbox"/> Other : List Classify Services	Lists one or all classified services
<input type="checkbox"/> Microsoft.Support/operationresults	
<input type="checkbox"/> Read : Get Operation Result	Gets the result of the asynchronous operation
<input type="checkbox"/> Microsoft.Support/operationsstatus	
<input type="checkbox"/> Read : Get Operation Status	Gets the status of the asynchronous operation
<input type="checkbox"/> Microsoft.Support/operations	

[Add](#) [Cancel](#)

- Select **Review + Create**, and then select **Create**.

Task 4: Monitor role assignments with the Activity Log

- In the portal locate the **az104-mg1** resource and select **Activity log**.
- Review the activities for role assignments.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information. The left sidebar contains a navigation menu with options like Overview, Subscriptions, Resource Groups, Resources, Activity Log, Access control (IAM), Governance, and Cost Management. The 'Activity Log' option is selected, leading to the 'az104-mg1 | Activity Log' page. This page shows a list of activities for the 'az104-mg1' management group. The 'Create role assignment' activity is highlighted. The right pane displays the details of this activity, including the resource path, operation name, time stamp, event initiator, message, role, and scope.

Create role assignment	
Wed Nov 26 2025 19:01:05 GMT+0500 (Pakistan Standard Time)	
+ New alert rule	
Summary JSON Change history (Change history is not applicable to this type of activity log)	
Resource	/providers/Microsoft.Management/managementGroups/az104-mg1/providers/Microsoft.Authorization/roleAssignments/c1e78d8f-8335-4d6b-87f5-8b439569ba14
Operation name	Create role assignment
Time stamp	Wed Nov 26 2025 19:01:05 GMT+0500 (Pakistan Standard Time)
Event initiated by	bsse2280155@szabist.pk
Message	-
Role	Virtual Machine Contributor
Scope	-