Shaheed Zulfikar Ali Bhutto Institute of Science and Technology

Department of Software Engineering

Bisma Saeed – 2280108

BSSE – 7A

Lab: 02 A

Administer Governance and Compliance

Lab 02a: Manage Subscriptions and RBAC

+ Task 1: Implement management groups.
+ Task 2: Review and assign a built-in Azure role.
+ Task 3: Create a custom RBAC role.
+ Task 4: Monitor role assignments with the Activity Log.

Task 1: Implement Management Groups

In this task, you will create and configure management groups. Management groups are used to logically organize and segment subscriptions. They allow for RBAC and Azure Policy to be assigned and inherited to other management groups and subscriptions. For example, if your organization has a dedicated support team for Europe, you can organize European subscriptions into a management group to provide the support staff access to those subscriptions (without providing individual access to all subscriptions). In our scenario everyone at the Help Desk will need to create a support request across all subscriptions.

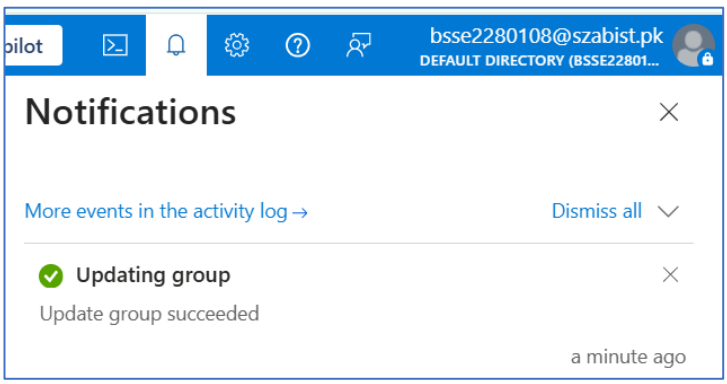
1. Sign in to the **Azure portal** - `https://portal.azure.com`.

2. Search for and select `Microsoft Entra ID`. In the **Manage** blade, select **Properties**.

3. Review the **Access management for Azure resources** area. Notice/read that you can manage access to all Azure subscriptions and management groups in the tenant.

4. Search for and select **Management groups**. On the **Management groups** blade, click **+ Create**.

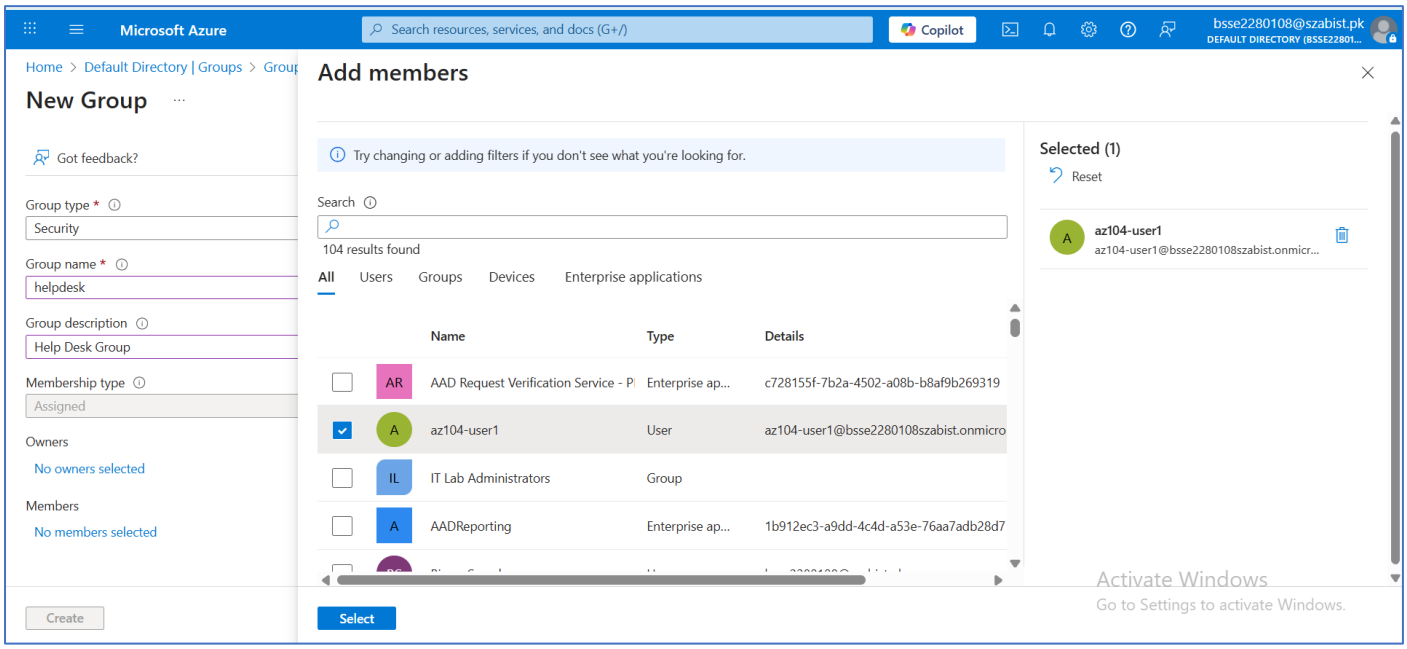
5. Create a management group with the following settings. Select **Submit** when you are done.

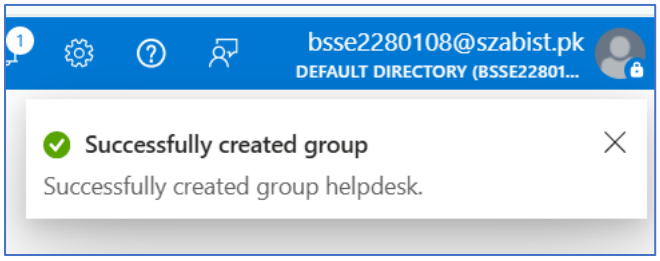


Task 2: Review and assign a built-in Azure role

In this task, you will review the built-in roles and assign the VM Contributor role to a member of the Help Desk. Azure provides a large number of [built-in roles](https://learn.microsoft.com/azure/role-based-access-control/built-in-roles).

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.





Assign “Virtual Machine Contributor” role to the helpdesk group

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

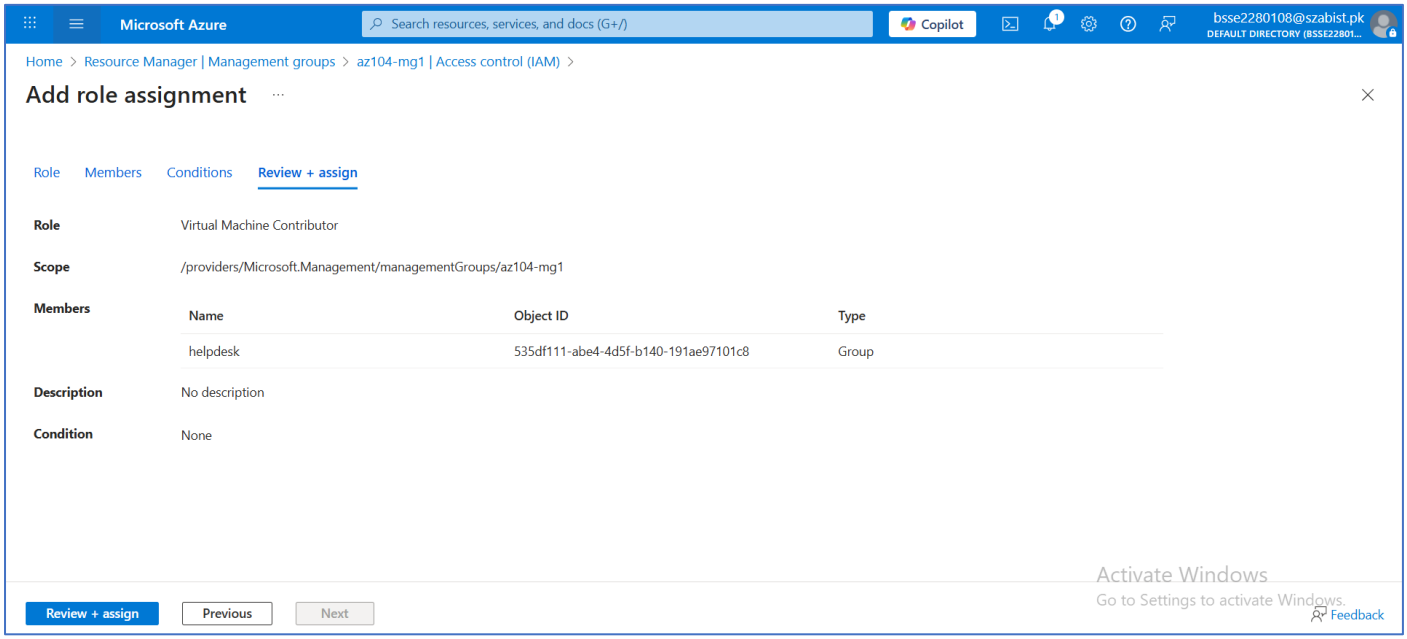
2. Select the **Access control (IAM)** blade, and then the **Roles** tab.

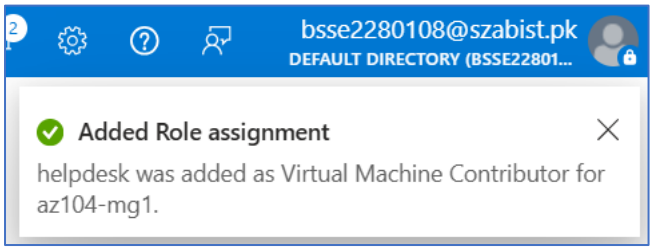
3. Scroll through the built-in role definitions that are available. **View** a role to get detailed information about the **Permissions**, **JSON**, and **Assignments**. You will often use *owner*, *contributor*, and *reader*.

4. Select **+ Add**, from the drop-down menu, select **Add role assignment**. On the **Add role assignment** blade, search for and select the **Virtual Machine Contributor**. The Virtual machine contributor role lets you manage virtual machines, but not access their operating system or manage the virtual network and storage account they are connected to. This is a good role for the Help Desk. Select **Next**.

5. On the **Members** tab, **Select Members**, Search for and select the `helpdesk` group. Click **Select**.

6. Click **Review + assign** twice to create the role assignment, Continue on the **Access control (IAM)** blade. On the **Role assignments** tab, confirm the **helpdesk** group has the **Virtual Machine Contributor** role.

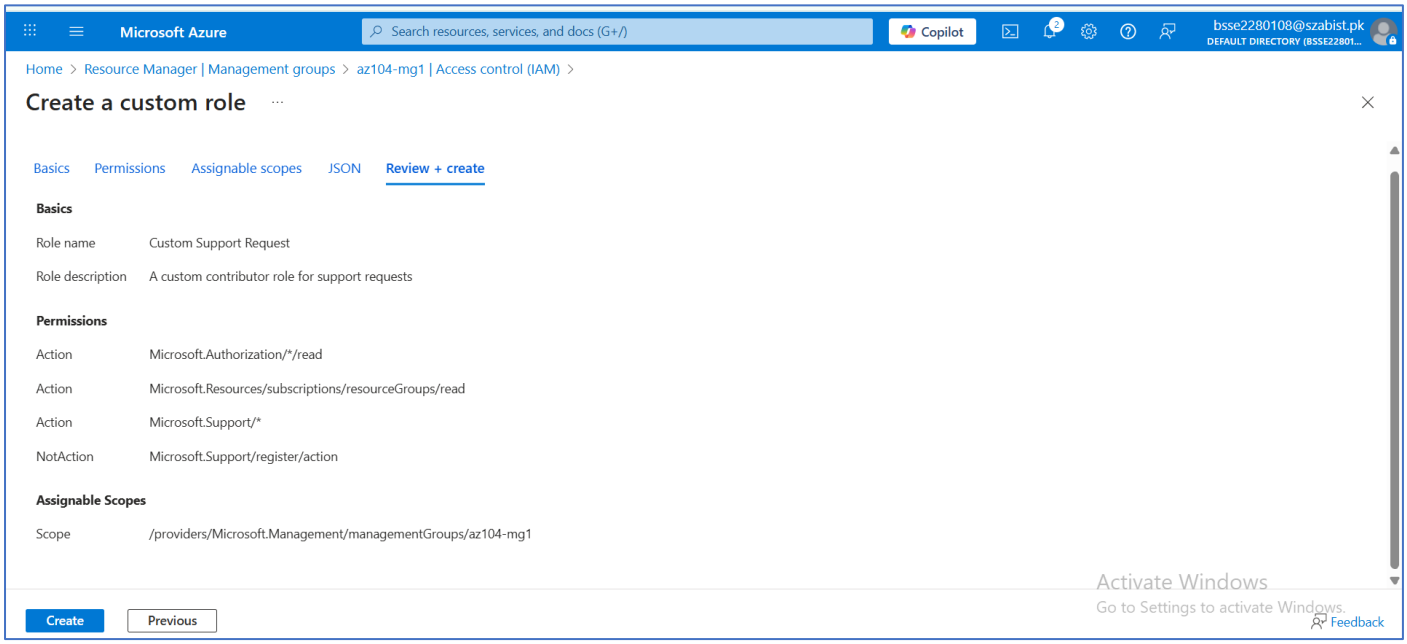


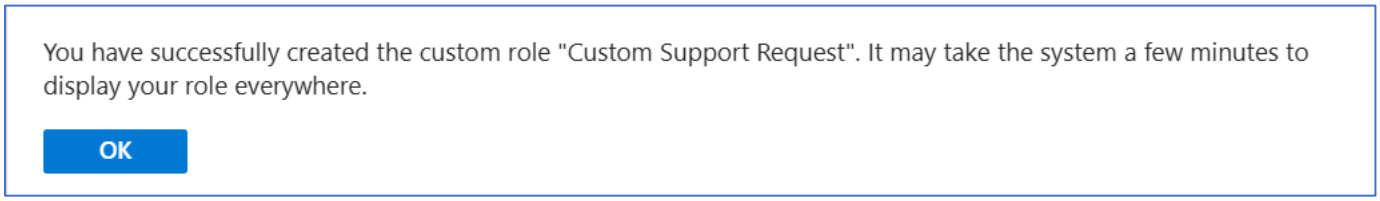


Task 3: Create a custom RBAC role

In this task, you will create a custom RBAC role. Custom roles are a core part of implementing the principle of least privilege for an environment. Built-in roles might have too many permissions for your scenario. We will also create a new role and remove permissions that are not necessary. Do you have a plan for managing overlapping permissions?

1. Continue working on your management group. Navigate to the **Access control (IAM)** blade.
2. Select **+ Add**, from the drop-down menu, select **Add custom role**.
3. On the Basics tab complete the configuration. For **Baseline permissions**, select **Clone a role**. In the **Role to clone** drop-down menu, select **Support Request Contributor**.
4. Select **Next** to move to the **Permissions** tab, and then select **+ Exclude permissions**.
5. In the resource provider search field, enter `.Support` and select **Microsoft.Support**.
6. In the list of permissions, place a checkbox next to **Other: Registers Support Resource Provider** and then select **Add**. The role should be updated to include this permission as a *NotAction*.
7. On the **Assignable scopes** tab, ensure your management group is listed, then click **Next**.
8. Review the JSON for the *Actions*, *NotActions*, and *AssignableScopes* that are customized in the role.
9. Select **Review + Create**, and then select **Create**.



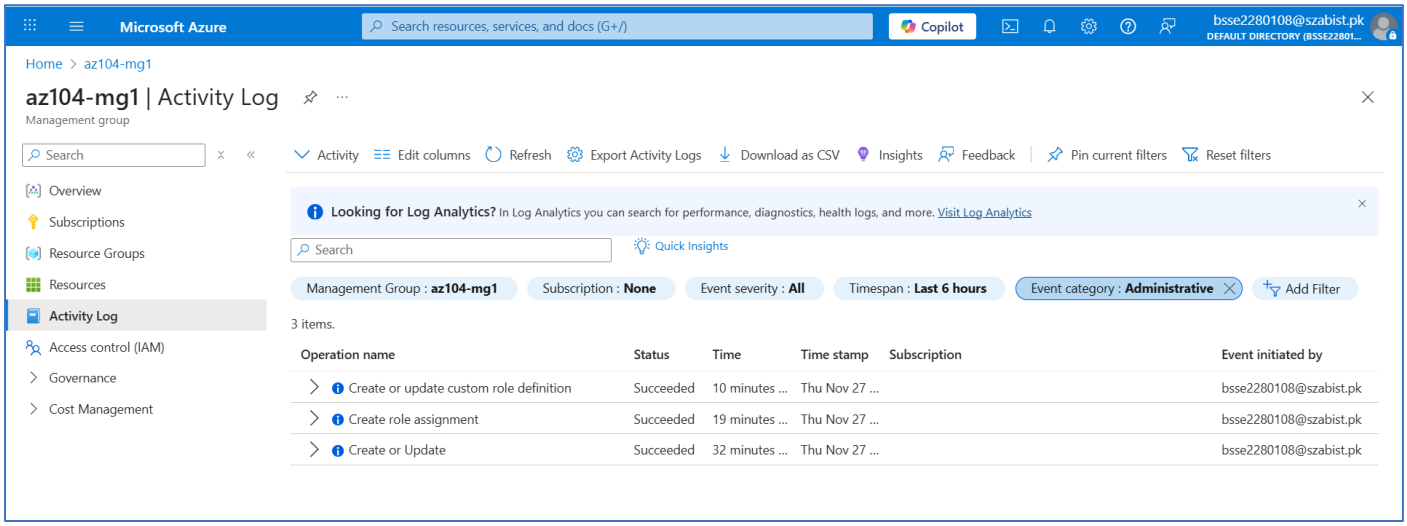


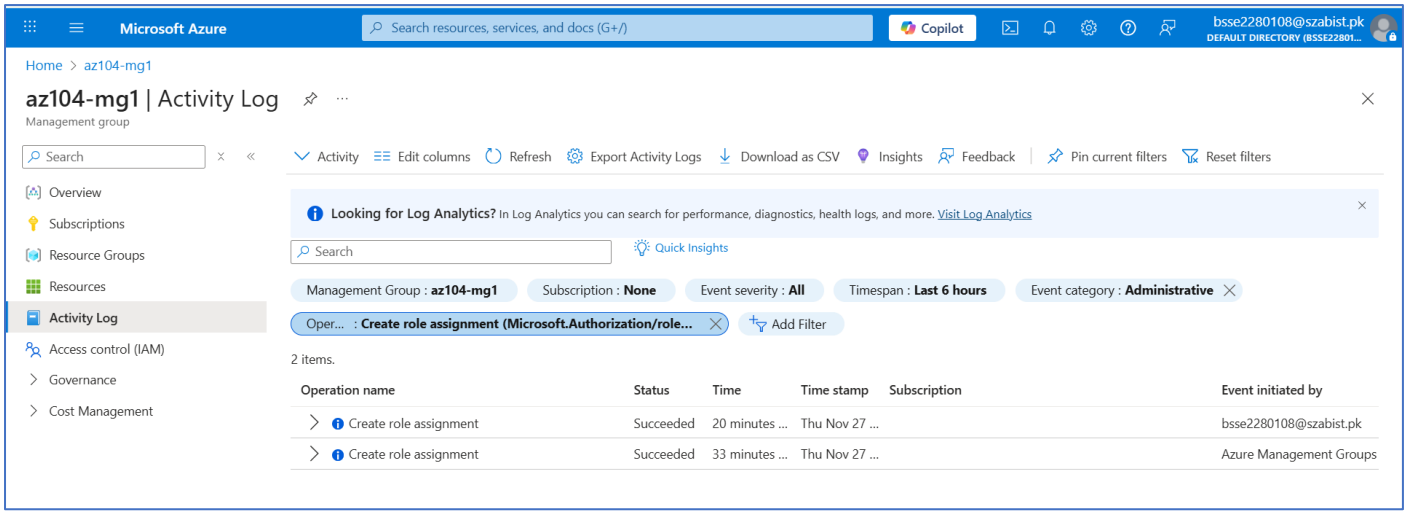
Task 4: Monitor role assignments with the Activity Log

In this task, you view the activity log to determine if anyone has created a new role.

1. In the portal locate the **az104-mg1** resource and select **Activity log**. The activity log provides insight into subscription-level events.

1. Review the activites for role assignments. The activity log can be filtered for specific operations.





Key takeaways

Congratulations on completing the lab. Here are the main takeaways for this lab.

+ Management groups are used to logically organize subscriptions.
+ The built-in root management group includes all the management groups and subscriptions.
+ Azure has many built-in roles. You can assign these roles to control access to resources.
+ You can create new roles or customize existing roles.
+ Roles are defined in a JSON formatted file and include *Actions*, *NotActions*, and *AssignableScopes*.
+ You can use the Activity Log to monitor role assignments.