Shaheed Zulfikar Ali Bhutto Institute of Science and Technology

Department of Software Engineering

Bisma Saeed – 2280108

BSSE – 7A

Lab: 02 B

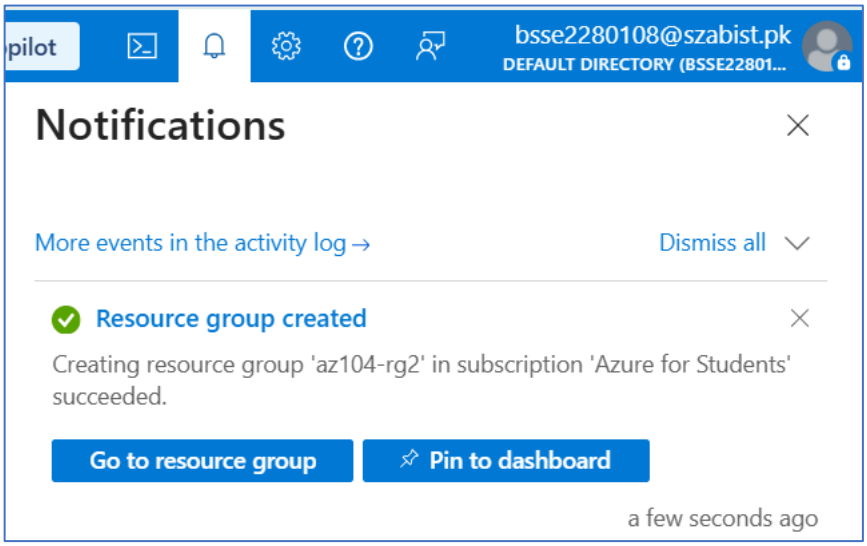
Administer Governance and Compliance

Lab 02b: Manage Governance via Azure Policy

+ Task 1: Create and assign tags via the Azure portal.
+ Task 2: Enforce tagging via an Azure Policy.
+ Task 3: Apply tagging via an Azure Policy.
+ Task 4: Configure and test resource locks.

Task 1: Assign tags via the Azure portal

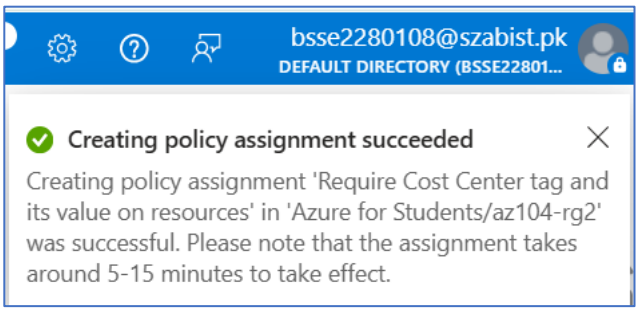
1. Sign in to the **Azure portal** - `https://portal.azure.com`.
2. Search for and select `Resource groups`.
3. From the Resource groups, select **+ Create**.
4. Select **Next** and move to the **Tags** tab. Provide information for a new tag.
5. Select **Review + Create**, and then select **Create**.



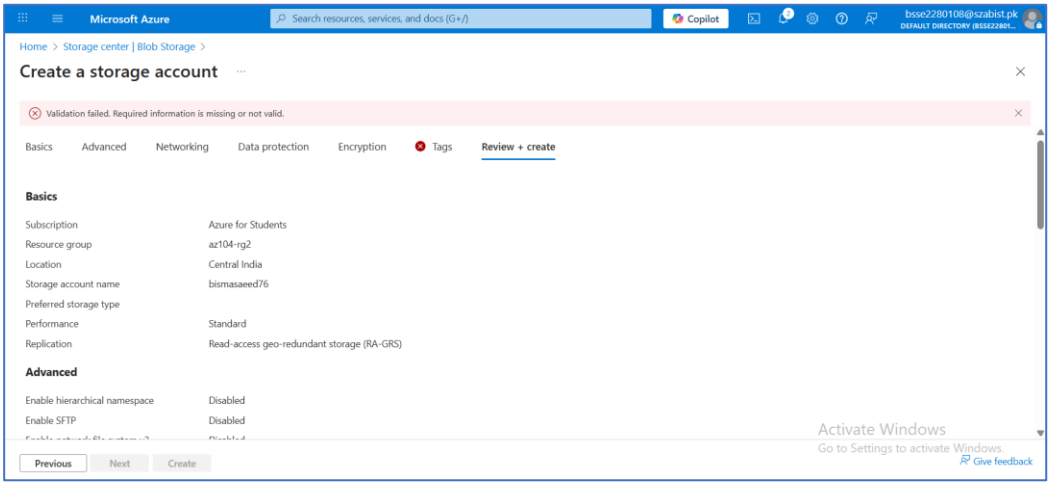
Task 2: Enforce tagging via an Azure Policy

In this task, you will assign the built-in *Require a tag and its value on resources* policy to the resource group and evaluate the outcome. Azure Policy can be used to enforce configuration, and in this case, governance, to your Azure resources.

1. In the Azure portal, search for and select `Policy`.
2. In the **Authoring** blade, select **Definitions**. Take a moment to browse through the list of [built-in policy definitions]
3. Search for the `Require a tag and its value on resources` built-in policy. Select the policy and take a minute to review the definition.
4. Select **Assign policy**. Specify the **Scope** by clicking the ellipsis button and selecting the following values. Click **Select** when you are done.
5. Configure the **Basics** properties of the assignment by specifying the following settings (leave others with their defaults):
6. Click **Next** and set **Parameters** to the following values:
7. Click **Next** and review the **Remediation** tab. Leave the **Create a Managed Identity** checkbox unchecked.
8. Click **Review + Create** and then click **Create**.
9. >**Note**: It might take between 5 and 10 minutes for the policy to take effect.

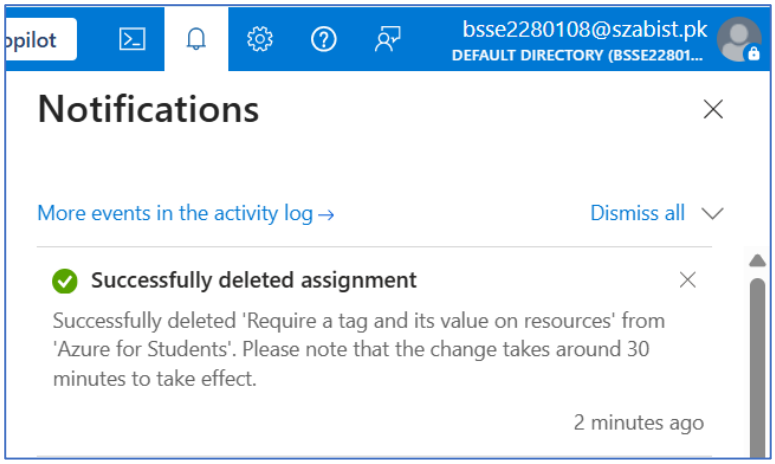


10. In the portal, search for and select `Storage Accounts`, and select **+ Create**.
11. On the **Basics** tab of the **Create storage account** blade, complete the configuration.
12. Select **Review** and then click **Create**.
13. You should receive a **Validation failed** message. View the message to identify the reason for the failure. Verify the error message states that the resource deployment was disallowed by the policy.

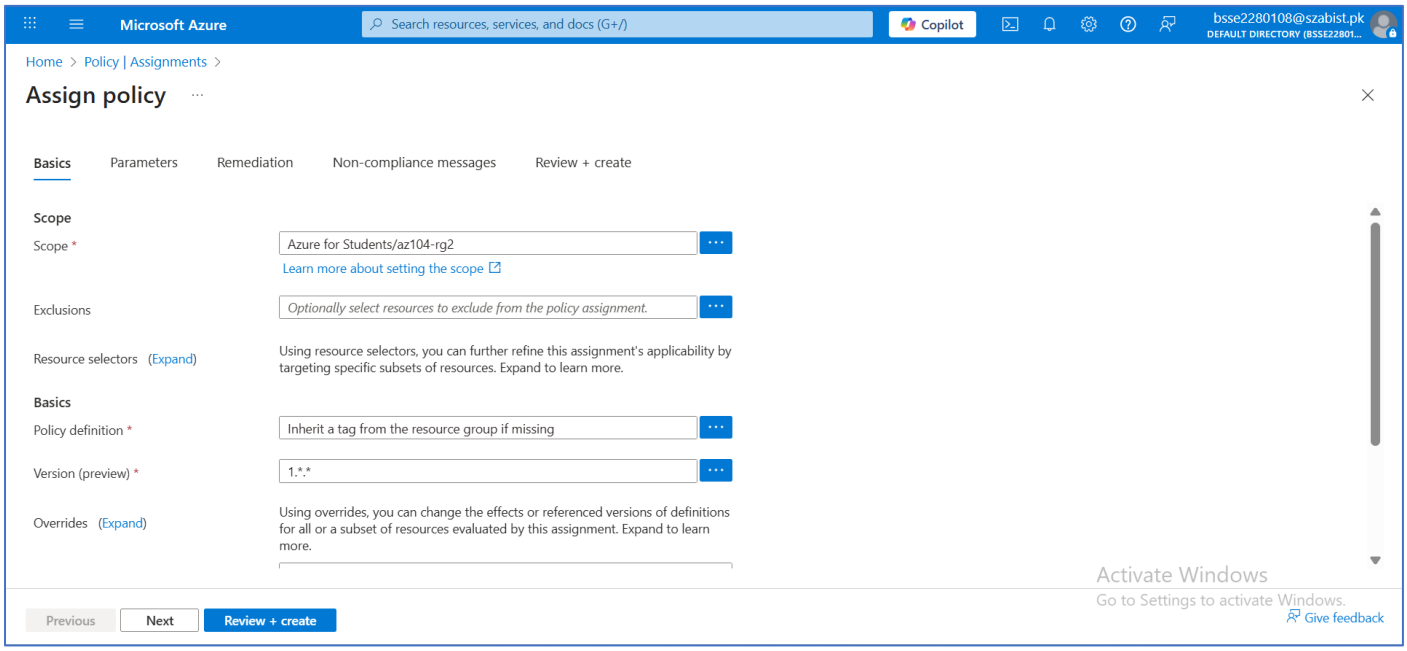


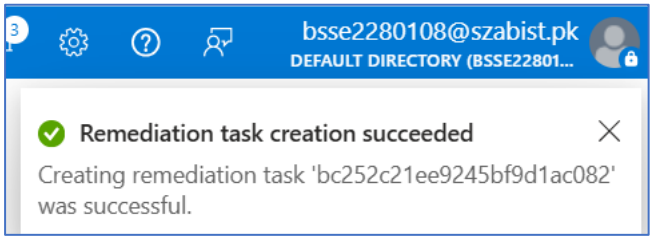
Task 3: Apply tagging via an Azure policy

1. In the Azure portal, search for and select `Policy`.
2. In the **Authoring** section, click **Assignments**.
3. In the list of assignments, click the ellipsis icon in the row representing the **Require a tag and its value on resources** policy assignment and use the **Delete assignment** menu item to delete the assignment.

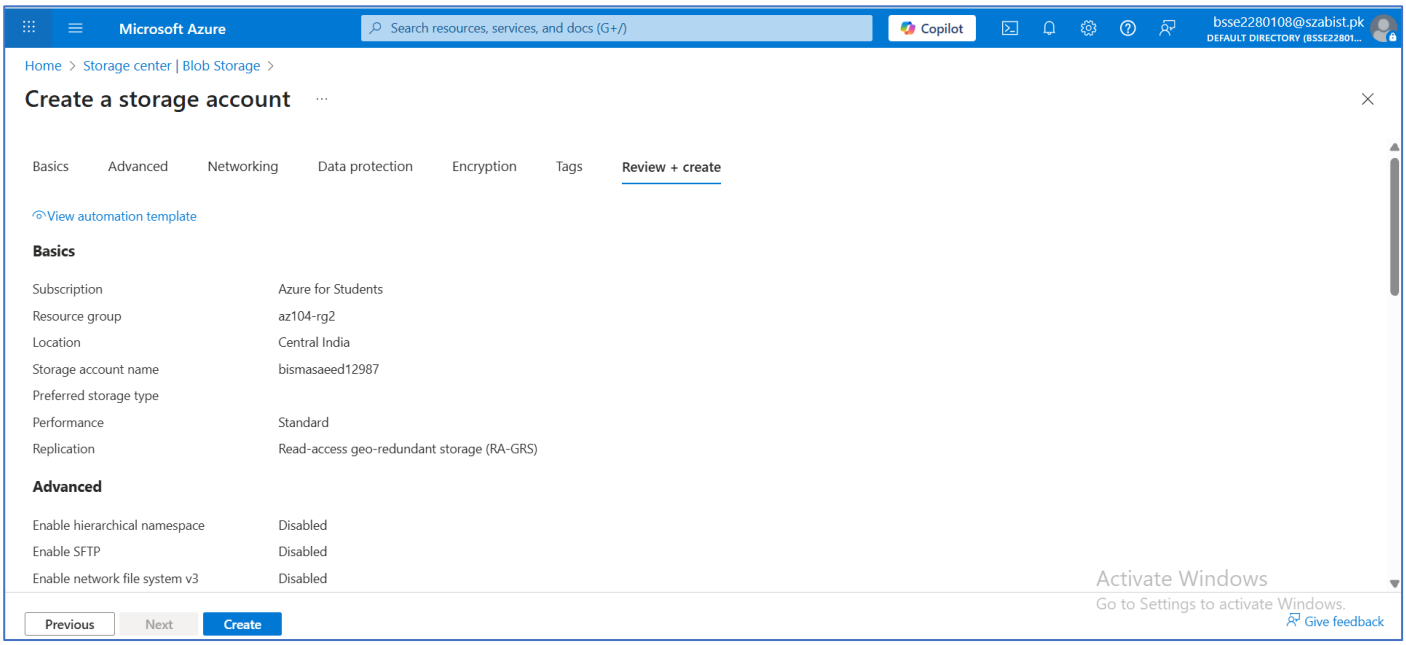


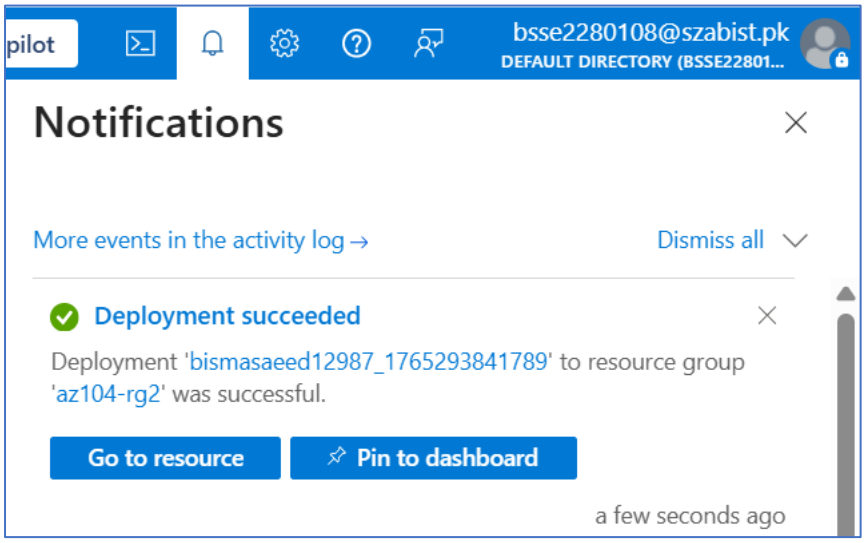
4. Click **Assign policy** and specify the **Scope** by clicking the ellipsis button and selecting the following values:
5. To specify the **Policy definition**, click the ellipsis button and then search for and select `Inherit a tag from the resource group if missing`.
6. Select **Add** and then configure the remaining **Basics** properties of the assignment.
7. Click **Next** and set **Parameters** to the following values:
8. Click **Next** and, on the **Remediation** tab, configure the following settings (leave others with their defaults):
9. Click **Review + Create** and then click **Create**. It might take between 5 and 10 minutes for the policy to take effect.

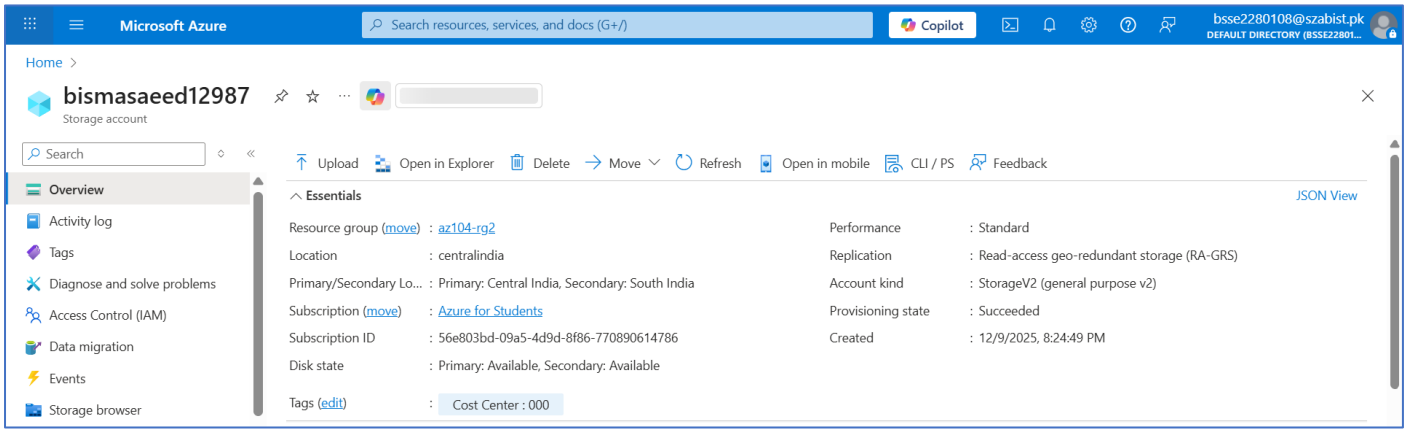


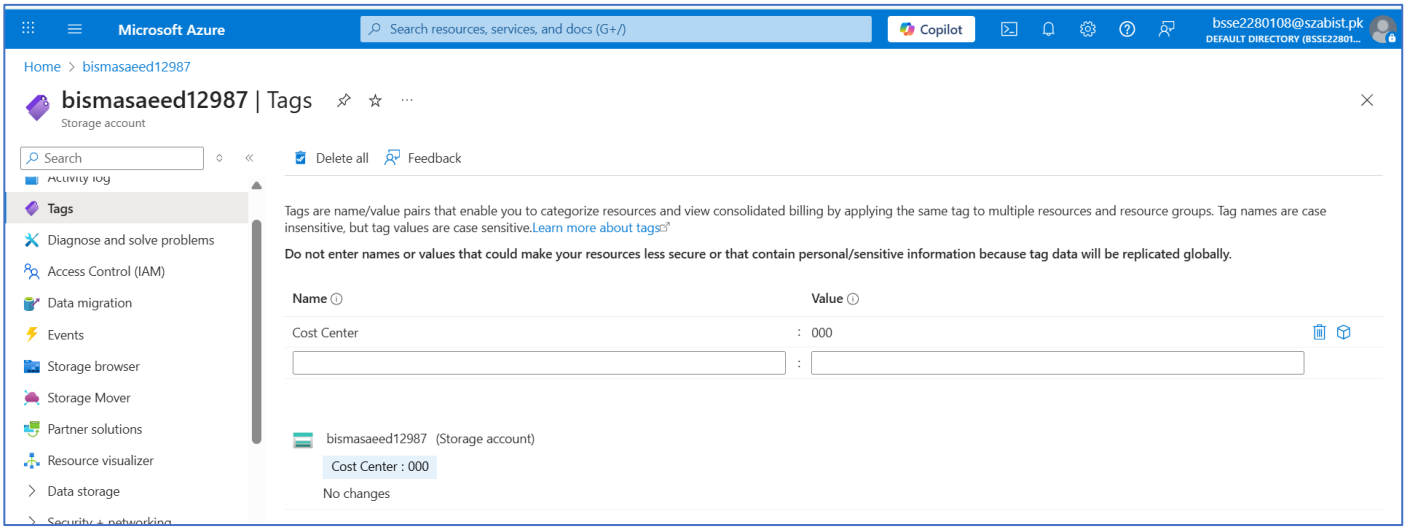


10. Search for and select `Storage Account` and click **+ Create**.
11. On the **Basics** tab of the **Create storage account** blade, verify that you are using the Resource Group that the Policy was applied to and specify the following settings (leave others with their defaults) and click **Review**:
12. Verify that this time the validation passed and click **Create**.





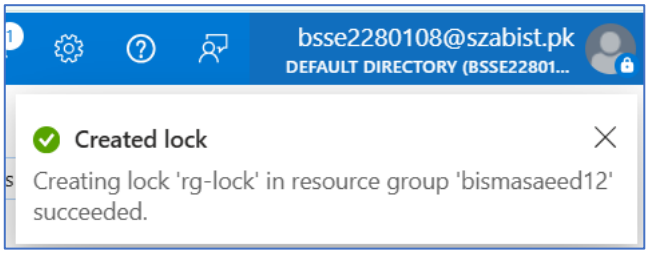



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
bsse2280108@szabist.pk
DEFAULT DIRECTORY (BSSE22801...
Home
bismasaeed12987
bismasaeed12987 | Tags
Storage account
Search
Tags
Diagnose and solve problems
Access Control (IAM)
Data migration
Events
Storage browser
Storage Mover
Partner solutions
Resource visualizer
Data storage
Delete all
Feedback
Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Tag names are case insensitive, but tag values are case sensitive.Learn more about tags
Do not enter names or values that could make your resources less secure or that contain personal/sensitive information because tag data will be replicated globally.
Name
Value
Cost Center
000
bismasaeed12987 (Storage account)
Cost Center : 000
No changes

Task 4: Configure and test resource locks

In this task, you configure and test a resource lock. Locks prevent either deletions or modifications of a resource.

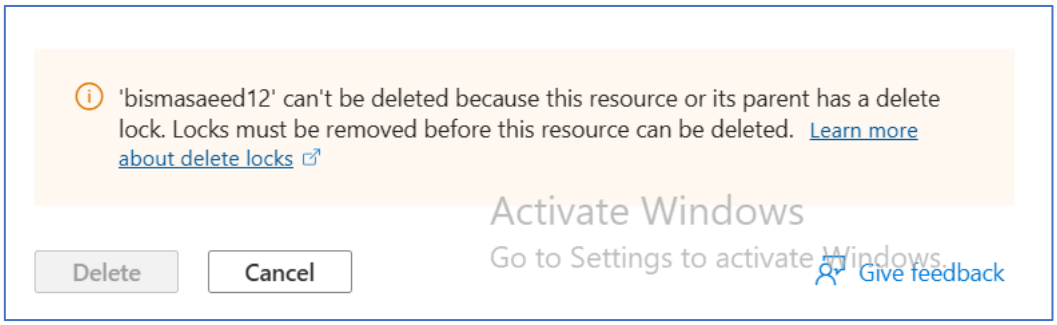
1. Search for and select your resource group.
2. In the **Settings** blade, select **Locks**.
3. Select **Add** and complete the resource lock information. When finished select **Ok**.



4. Navigate to the resource group **Overview** blade, and select **Delete resource group**.
5. In the **Enter resource group name to confirm deletion** textbox provide the resource group name, `az104-rg2`. Notice you can copy and paste the resource group name.
6. Notice the warning: Deleting this resource group and its dependent resources is a permanent action and cannot be undone. Select **Delete**.

You should receive a notification denying the deletion.

7.



Key takeaways

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

+ Azure tags are metadata that consists of a key-value pair. Tags describe a particular resource in your environment. In particular, tagging in Azure enables you to label your resources in a logical manner.
+ Azure Policy establishes conventions for resources. Policy definitions describe resource compliance conditions and the effect to take if a condition is met. A condition compares a resource property field or a value to a required value. There are many built-in policy definitions and you can customize the policies.
+ The Azure Policy remediation task feature is used to bring resources into compliance based on a definition and assignment. Resources that are non-compliant to a modify or deployIfNotExist definition assignment, can be brought into compliance using a remediation task.
+ You can configure a resource lock on a subscription, resource group, or resource. The lock can protect a resource from accidental user deletions and modifications. The lock overrides any user permissions.
+ Azure Policy is pre-deployment security practice. RBAC and resource locks are post-deployment security practice.