

**CANTON WEKE OTIENO**

**SECURITY ENGINEER TRACK**

**STUDENT TRACKING NUMBER; ADC-SE01-24010**

**CYBER SHUJAA**

**INSTRUCTOR: Dr. Paula**

## **LAB 02B - MANAGE GOVERNANCE VIA AZURE POLICY**

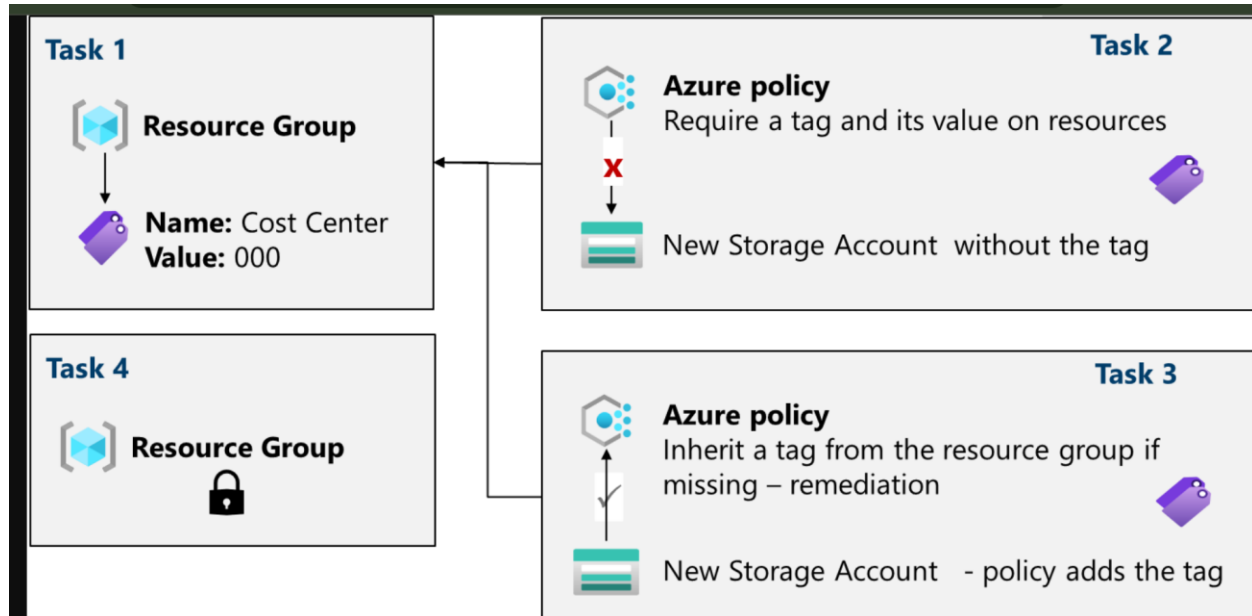
### **Introduction**

An extensive examination of the efficient implementation and management of governance policies within Microsoft Azure is covered by "LAB 02B - Manage Governance via Azure Policy". In order to maintain a safe and legal cloud environment, the lab concentrated on the actual use of Azure tags, policy definitions, remediation tasks, and resource locks. Azure tags, which are made up of key-value pairs, make it possible to logically classify and arrange resources, which makes management and analysis easier. Azure Policy ensures that resources adhere to organizational standards by establishing and enforcing compliance requirements. By enabling automatic rectification of non-compliant resources, the remediation task feature encourages ongoing adherence to policies. Resource locks also improve the environment's overall security by acting as a buffer against unintentional additions and deletions. I received invaluable practical experience from this lab.

The "LAB 02B - Manage Governance via Azure Policy" taught me that pre- and post-deployment processes work together to establish successful governance in Azure. Azure tags are essential for logical resource organization, which facilitates resource management and tracking. Resources are guaranteed to continuously fulfill organizational standards and legal requirements when Azure Policy is used to create compliance criteria and remediation tasks. Governance procedures are streamlined and the chance of human error is decreased by this automatic compliance testing and correction. Resource locks also provide an extra crucial degree of protection by shielding resources from inadvertent modifications. The lab emphasized that both

proactive and reactive actions are necessary to ensure a safe, orderly, and compliant Azure environment. It also stressed the significance of integrating these governance tools.

## ARCHITECTURE DIAGRAM



### TASK 1: ASSIGN TAGS VIA THE AZURE PORTAL

According to the Cloud Adoption Framework and Microsoft Well-Architected Framework, tags are an essential part of a governance approach. You may quickly find resource owners, sunset dates, group contacts, and other name/value pairs that are important to your company by using tags.

#### Instructions on how to create a resource group

- Sign in to the Azure portal - <https://portal.azure.com>.
- Search for and select Resource groups.
- From the Resource groups, select + Create.
- Select Next: Tags and create a new tag.

- Select Review + Create, and then select Create.

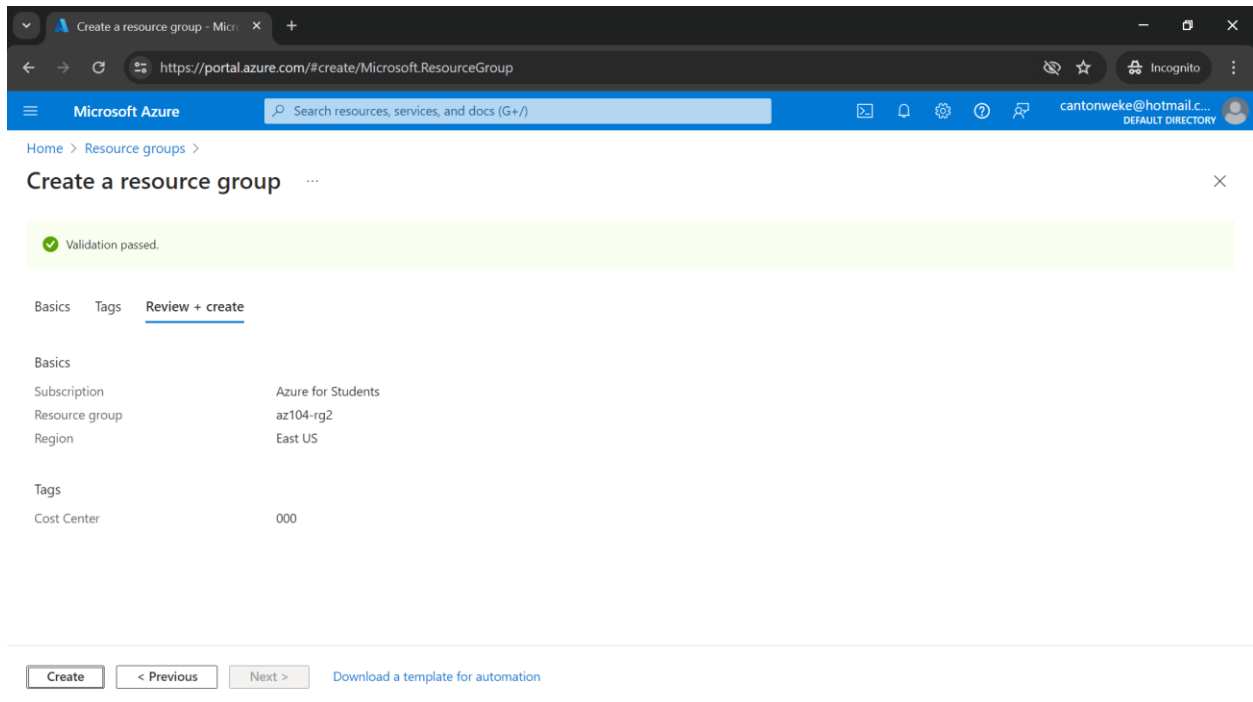
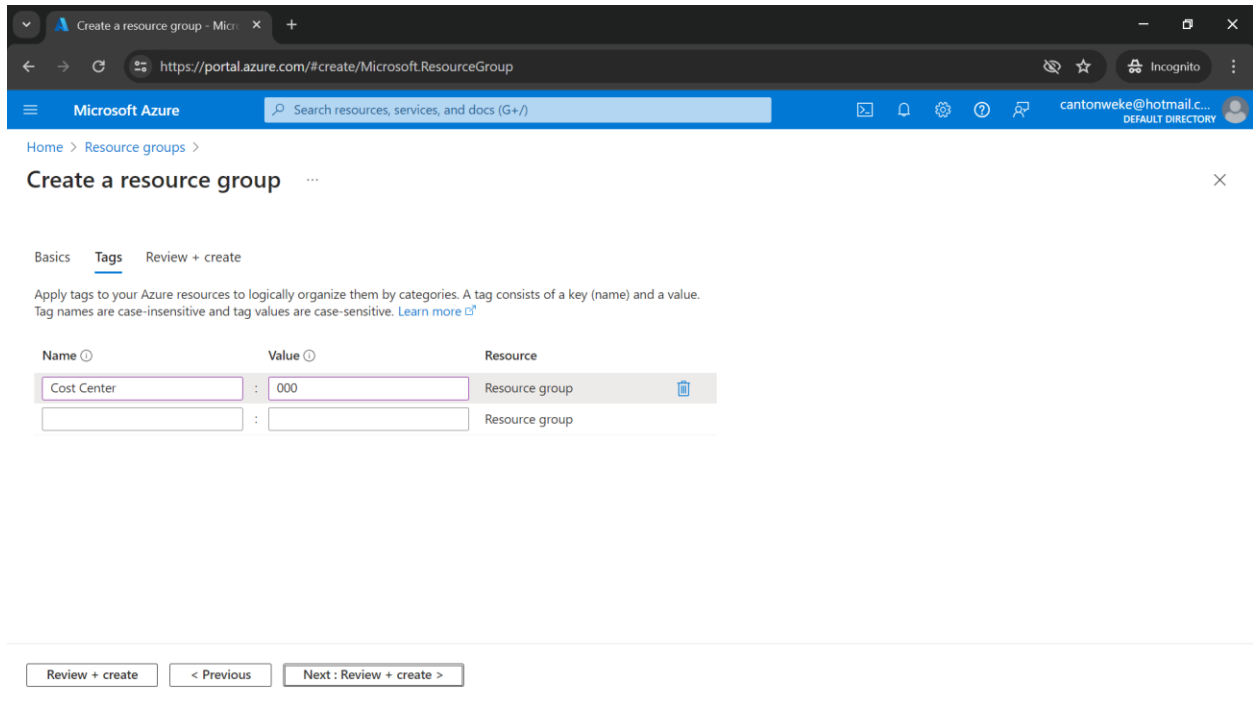
## Screenshot showing how to create the resource groups

The screenshot shows the Microsoft Azure portal interface for creating a resource group. The browser address bar displays `https://portal.azure.com/#create/Microsoft.ResourceGroup`. The page title is "Create a resource group". The "Basics" tab is selected, showing the following details:

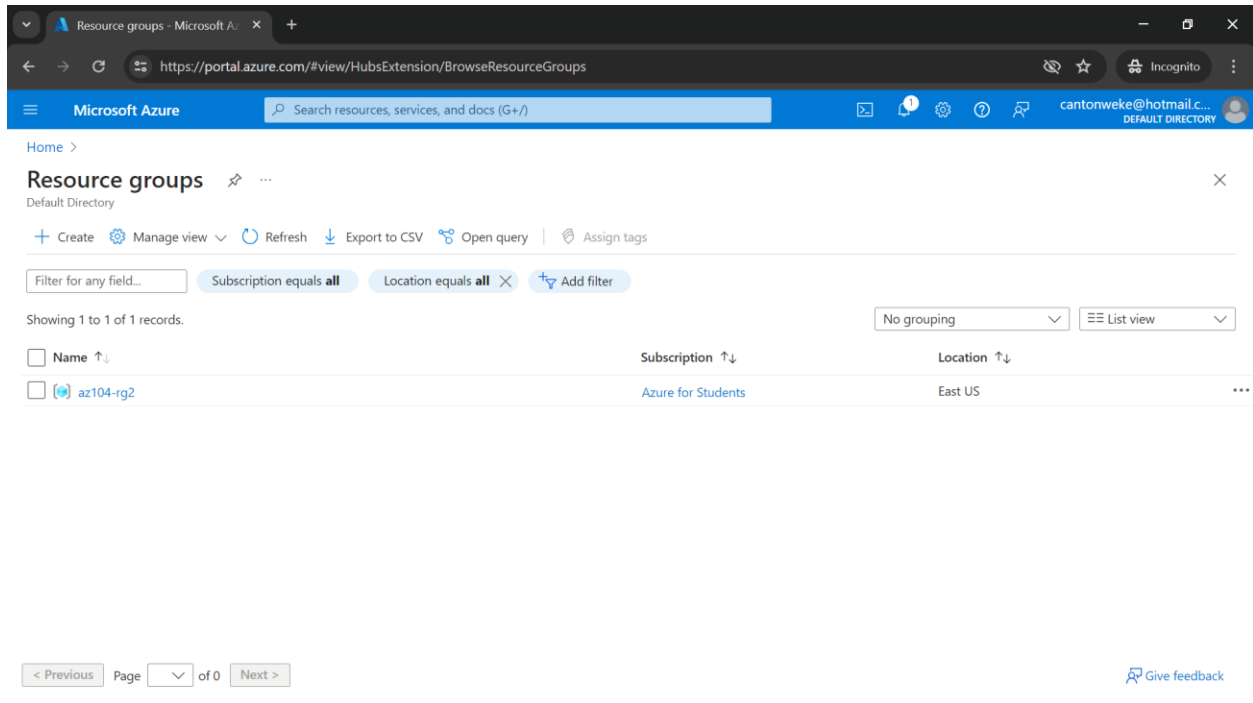
- Project details**
  - Subscription: Azure for Students
  - Resource group: az104-rg2
- Resource details**
  - Region: (US) East US

At the bottom of the form, there are three buttons: "Review + create", "< Previous", and "Next : Tags >".

## Tags

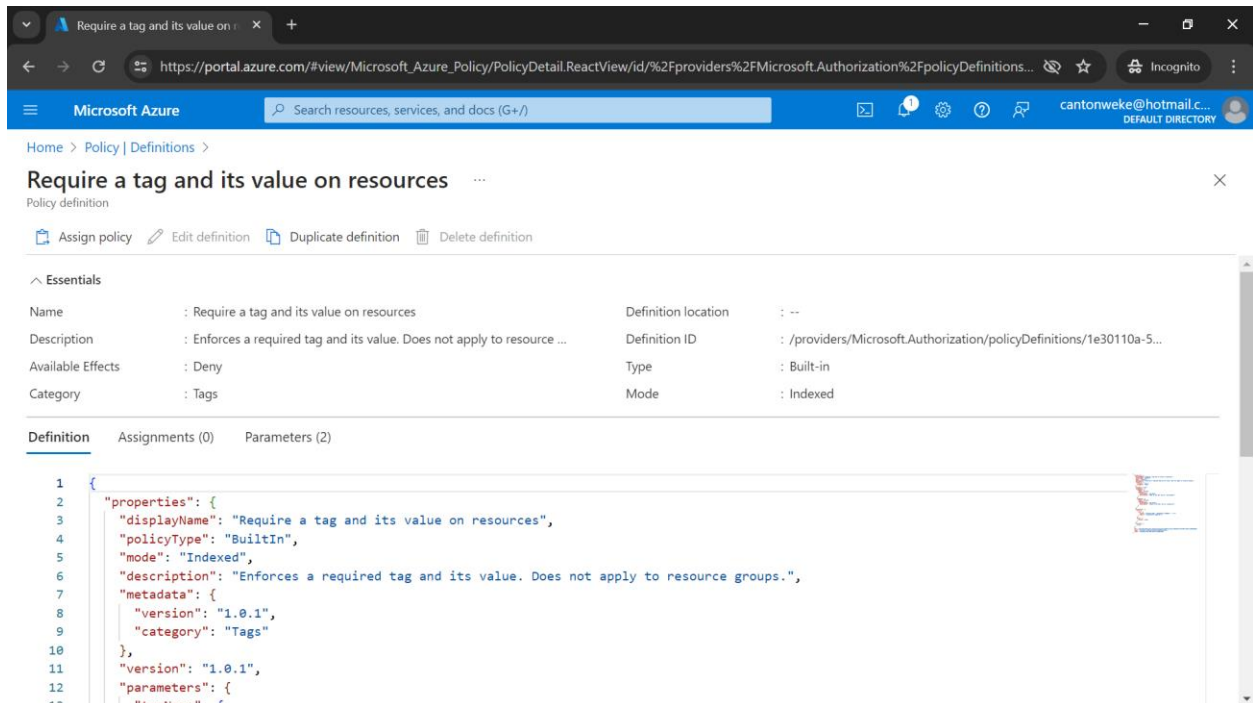


**screenshot showing created Resource group**



## Task 2: Enforce tagging via an Azure Policy

### Screenshot



Scope - Microsoft Azure

https://portal.azure.com/#view/Microsoft\_Azure\_Policy/CreateAssignmentBladeV2/definitionId/%2Fproviders%2FMicrosoft.Authorization%2Fpol...

Microsoft Azure

Search resources, services, and docs (G+)

Home > Policy | Definitions > Require a tag and its value on resources >

### Require a tag and its value on resources

Assign policy

Basics Advanced Parameters Remediation Non-compliance messages Review + create

**Scope** [Learn more about setting the scope \\*](#)

Scope

Exclusions

Optionally select resources to exclude from the policy assignment.

**Basics**

Policy definition

Require a tag and its value on resources

Assignment name \*

Require a tag and its value on resources

Description

Require Cost Center tag with default value for all resources in the resource group

Review + create Cancel Previous Next

Scope

Management Group

Tenant Root Group (a94bfb3d-507f-4529-baf9-e1d304c44c8f)

Subscription

Azure for Students

Resource Group

az104-rg2

Select Cancel Clear All Selections

Configure the Basics properties of the assignment by specifying the following settings (leave others with their defaults): Screenshot

Require a tag and its value on resources

https://portal.azure.com/#view/Microsoft\_Azure\_Policy/CreateAssignmentBladeV2/definitionId/%2Fproviders%2FMicrosoft.Authorization%2Fpol...

Microsoft Azure

Search resources, services, and docs (G+)

Home > Policy | Definitions > Require a tag and its value on resources >

### Require a tag and its value on resources

Assign policy

Basics Advanced Parameters Remediation Non-compliance messages Review + create

**Scope** [Learn more about setting the scope \\*](#)

Scope

Azure for Students/az104-rg2

Exclusions

Optionally select resources to exclude from the policy assignment.

**Basics**

Policy definition

Require a tag and its value on resources

Assignment name \*

Require Cost Center tag with Default value

Description

Require Cost Center tag with default value for all resources in the resource group

Review + create Cancel Previous Next

Click Next twice and set Parameters to the following values:

Setting	Value
Tag Name	Cost Center
Tag Value	000

Screenshot

The screenshot shows the Microsoft Azure portal interface. The browser address bar displays the URL: [https://portal.azure.com/#view/Microsoft\\_Azure\\_Policy/CreateAssignmentBladeV2/definitionId/%2Fproviders%2FMicrosoft.Authorization%2Fpol...](https://portal.azure.com/#view/Microsoft_Azure_Policy/CreateAssignmentBladeV2/definitionId/%2Fproviders%2FMicrosoft.Authorization%2Fpol...). The page title is "Require a tag and its value on resources". Below the title, there are tabs for "Basics", "Advanced", "Parameters", "Remediation", "Non-compliance messages", and "Review + create". The "Parameters" tab is currently selected. Under this tab, there is a search bar labeled "Search by parameter ..." and a checkbox labeled "Only show parameters that need input or review" which is checked. Below the search bar, there are two input fields: "Tag Name" with the value "Cost Center" and "Tag Value" with the value "000". Both fields have a green checkmark icon to their right. At the bottom of the page, there are four buttons: "Review + create" (highlighted in blue), "Cancel", "Previous", and "Next".

In the portal, search for and select Storage Account, and select + Create.

On the Basics tab of the Create storage account blade, complete the configuration.

Select Review and then click Create.



Create a storage account - Microsoft Azure

Home > Storage accounts >

## Create a storage account

manage your storage account together with other resources.

Subscription \* Azure for Students

Resource group \* az104-rg2 [Create new](#)

**Instance details**

Storage account name \* domestic1

Region \* (US) East US [Deploy to an Azure Extended Zone](#)

Performance \* ☒ Standard: Recommended for most scenarios (general-purpose v2 account)  
☐ Premium: Recommended for scenarios that require low latency.

Redundancy \* Geo-redundant storage (GRS)  
☒ Make read access to data available in the event of regional unavailability.

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

[Give feedback](#)

Screenshot showing validation error message.

Create a storage account - Microsoft Azure

Home > Storage accounts >

## Create a storage account

**Validation failed** [View error details](#)

**Basics**

Subscription	Azure for Students
Resource group	az104-rg2
Location	East US
Storage account name	domestic1
Performance	Standard
Replication	Read-access geo-redundant storage (RA-GRS)

**Advanced**

Enable hierarchical namespace	Disabled
Enable SFTP	Disabled
Enable network file system v3	Disabled
Allow cross-tenant replication	Disabled
Access tier	Hot

[Previous](#) [Next](#) [Create](#)

[Give feedback](#)

The screenshot shows the Microsoft Azure portal interface. The main content area displays the 'Create a storage account' form. A validation error is highlighted at the top: 'Validation failed. View error details →'. Below this, a table lists various storage account settings and their status:

Setting	Status
Blob soft delete	Enabled
Blob retainment period in days	7
Container soft delete	Enabled
Container retainment period in days	7
File share soft delete	Enabled
File share retainment period in days	7
Versioning	Disabled
Blob change feed	Disabled
Version-level immutability support	Disabled

Below the table, there is an 'Encryption' section with the following settings:

Setting	Status
Encryption type	Microsoft-managed keys (MMK)
Enable support for customer-managed keys	Blobs and files only
Enable infrastructure encryption	Disabled

At the bottom of the form are buttons for 'Previous', 'Next', and 'Create'. On the right side, the 'Errors' pane is open, showing a 'Summary' tab. The error details are as follows:

**ERROR DETAILS**

Resource 'domestic1' was disallowed by policy. (Code: RequestDisallowedByPolicy)

Policy: Require Cost Center tag with Default value

Below the error details, there is a 'WAS THIS HELPFUL?' section with thumbs up and thumbs down icons. Further down, there are 'Troubleshooting Options' including a link to 'New Support Request'. At the bottom of the errors pane, there is a 'Give Feedback' section with a link to 'Tell us about your experience with the ARM Errors page'.

### TASK 3: APPLY TAGGING VIA AN AZURE POLICY

#### Instructions and steps to complete the task.

- In the Azure portal, search for and select Policy.
- In the Authoring section, click Assignments.
- In the list of assignments, click the ellipsis icon in the row representing the Require Cost Center tag with Default value policy assignment and use the Delete assignment menu item to delete the assignment.
- Click Assign policy and specify the Scope by clicking the ellipsis button.

## Screenshot

This screenshot shows the 'Policy | Assignments' page in the Microsoft Azure portal. The left-hand navigation pane includes links for Overview, Getting started, Compliance, Remediation, Events, Authoring, Definitions, Assignments (which is highlighted), and Exemptions. The main content area features a search bar and filters for 'Scope: Azure for Students' and 'Definition type: All definition types'. It displays summary statistics: 1 Total Assignment, 0 Initiative Assignments, and 1 Policy Assignment. Below this, a table lists the assignments with columns for 'Assignment name', 'Scope', and 'Type'. One assignment is listed: 'Require Cost Center tag with Default value' with a scope of 'Azure for Students/az104-rg2' and a type of 'Policy'.

Assignment name	Scope	Type
Require Cost Center tag with Default value	Azure for Students/az104-rg2	Policy

This screenshot shows the 'Assign policy' wizard in the Microsoft Azure portal. The 'Basics' tab is selected, showing fields for 'Scope' (set to 'Azure for Students'), 'Exclusions', 'Policy definition', 'Assignment name', and 'Description'. A 'Scope' sidebar is open on the right, showing the hierarchy: Management Group (Tenant Root Group), Subscription (Azure for Students), and Resource Group (az104-rg2). At the bottom, there are buttons for 'Review + create', 'Cancel', 'Previous', 'Next', 'Select', and 'Clear All Selections'.

Select Add and then configure the remaining Basics properties of the assignment.

Assign policy

Optionally select resources to exclude from the policy assignment.

**Basics**

Policy definition \*  
Inherit a tag from the resource group if missing

Assignment name \* ⓘ  
Inherit a tag from the resource group if missing

Description  
Inherit the Cost Center tag and its value 000 from the resource group if missing

Policy enforcement ⓘ  
**Enabled** Disabled

**Review + create** Cancel Previous Next

Policy | Assignments

Search

Assign policy Assign initiative Refresh

Filter by name or ID...

Scope: Azure for Students Definition type: All definition types

Total Assignments ⓘ Initiative Assignments ⓘ Policy Assignments ⓘ

1 0 1

Assignment name ⓘ	Scope ⓘ	Type ⓘ
Inherit a tag from the resource group if missing	Azure for Students/az104-rg2	Policy

https://portal.azure.com/#view/Microsoft\_Azure\_Policy/PolicyMenuBlade/~-/Assignments

Search for and select Storage Account, and click + Create.

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:

## Screenshot

The screenshot shows the 'Create a storage account' blade in the Azure portal. The browser address bar shows the URL: <https://portal.azure.com/#create/Microsoft.StorageAccount-ARM>. The page title is 'Create a storage account'. Below the title, there is a note: 'Pricing: The cost of your storage account depends on the usage and the options you choose below. [Learn more about Azure storage accounts](#)'. The 'Project details' section includes a description: 'Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.' It has two dropdown menus: 'Subscription' (set to 'Azure for Students') and 'Resource group' (set to 'az104-rg2'). There is a 'Create new' link below the resource group dropdown. The 'Instance details' section includes a text input for 'Storage account name' (set to 'domestic2'), a dropdown for 'Region' (set to '(US) East US'), and a link 'Deploy to an Azure Extended Zone'. The 'Performance' section has a radio button selected for 'Standard: Recommended for most scenarios (general-purpose v2 account)'. At the bottom, there are three buttons: 'Previous', 'Next', and 'Review + create'. A 'Give feedback' link is also present.

Create a storage account - Microsoft Azure

Home > Storage accounts >

### Create a storage account

Pricing: The cost of your storage account depends on the usage and the options you choose below. [Learn more about Azure storage accounts](#)

**Project details**

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription \* Azure for Students

Resource group \* az104-rg2 [Create new](#)

**Instance details**

Storage account name \* domestic2

Region \* (US) East US [Deploy to an Azure Extended Zone](#)

Performance \* ☒ Standard: Recommended for most scenarios (general-purpose v2 account)

[Previous](#) [Next](#) [Review + create](#) [Give feedback](#)

## Screenshot showing created storage account

The screenshot displays the Microsoft Azure portal interface. The browser address bar shows the URL: <https://portal.azure.com/#view/HubsExtension/DeploymentDetailsBlade/~/overview/id/%2Fsubscriptions%2F4f3c0128-9784-4d96-90c6-34c866...>. The page title is "domestic2\_1717076875454 | Overview". The left sidebar contains a search bar and a navigation menu with "Overview" (selected), "Inputs", "Outputs", and "Template". The main content area features a green checkmark icon and the text "Your deployment is complete". Below this, deployment details are listed: "Deployment name: domestic2\_17170768...", "Subscription: Azure for Students", "Resource group: az104-rg2", "Start time: 5/30/2024, 4:48:38 PM", and "Correlation ID: 950c328c-104c-4ebd-af39-82ac4bf5ab9f". A "Go to resource" button is present. The right sidebar contains three sections: "Cost Management" with a link to "Set up cost alerts", "Microsoft Defender for Cloud" with a link to "Go to Microsoft Defender for Cloud", and "Free Microsoft tutorials" with a link to "Start learning today". At the bottom of the right sidebar, it says "Work with an expert" and "Azure experts are service provider partners".

Home > domestic2\_1717076875454 | Overview

Deployment

Search

Overview

Inputs

Outputs

Template

✓ Your deployment is complete

Deployment name: domestic2\_17170768... Start time: 5/30/2024, 4:48:38 PM  
Subscription: Azure for Students Correlation ID: 950c328c-104c-4ebd-af39-82ac4bf5ab9f  
Resource group: az104-rg2

Deployment details

Next steps

Go to resource

Give feedback

Tell us about your experience with deployment

Cost Management

Get notified to stay within your budget and prevent unexpected charges on your bill.  
Set up cost alerts >

Microsoft Defender for Cloud

Secure your apps and infrastructure  
Go to Microsoft Defender for Cloud >

Free Microsoft tutorials

Start learning today >

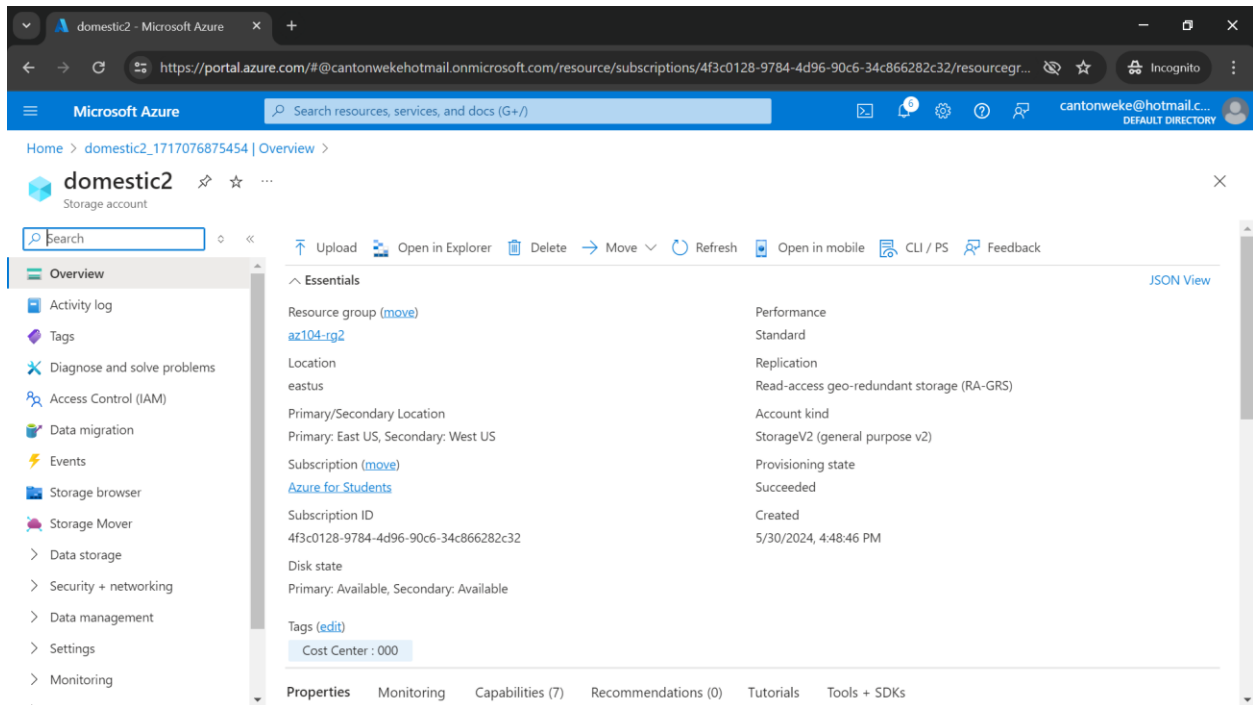
Work with an expert

Azure experts are service provider partners

Once the new storage account is provisioned, click Go to resource.

On the Tags blade, note that the tag Cost Center with the value 000 has been automatically assigned to the resource.

## Screenshot



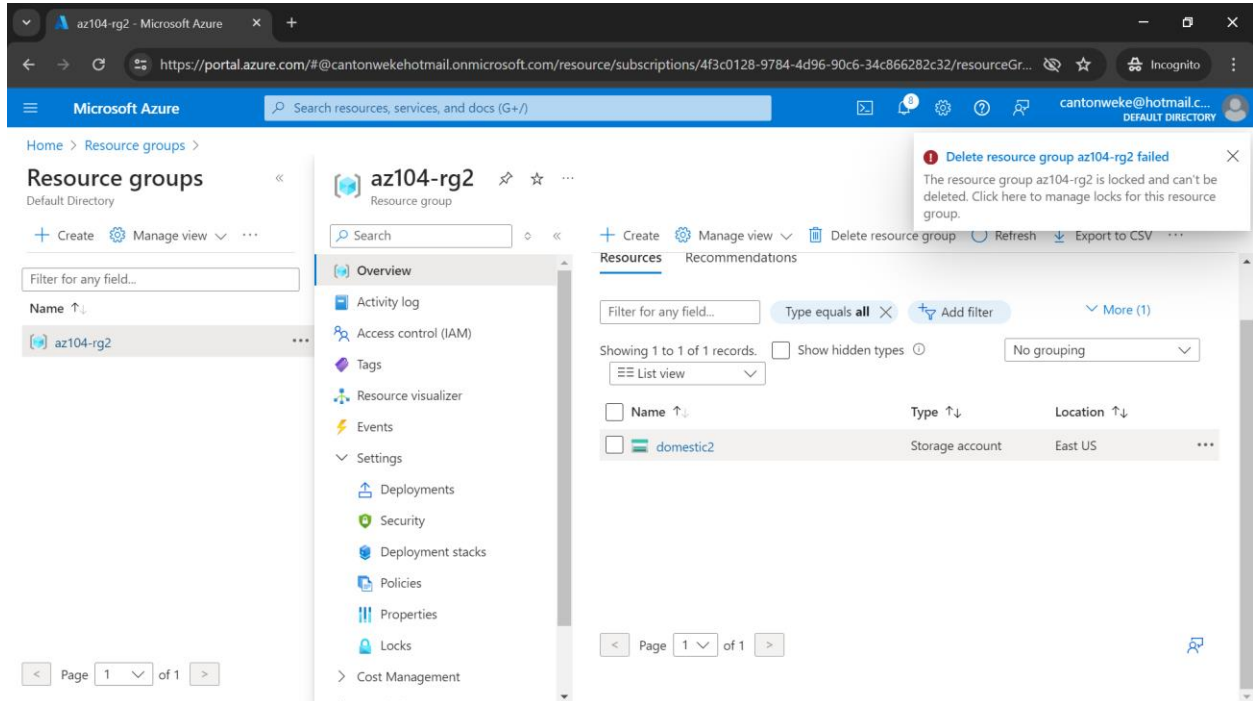
## TASK 4: CONFIGURE AND TEST RESOURCE LOCKS

### Instructions

- Search for and select your resource group.
- In the Settings blade, select Locks.
- Select Add and complete the resource lock information. When finished select Ok.
- Navigate to the resource group Overview blade, and select Delete resource group.
- 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.

- 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.

## Screenshot





## CONCLUSION

As a conclusion, the "LAB 02B - Manage Governance via Azure Policy" has brought attention to the importance of putting in place sensible governance practices in Microsoft Azure environments. In order to properly organize and describe resources and facilitate straightforward identification and management throughout a complex infrastructure, Azure tags—which are composed of key-value pairs—play a crucial role. Organizations can reorganize their resource management procedures and improve tracking and analysis of expenses, performance indicators, and utilization by properly naming their resources.

Resource management conventions are established and enforced in large part by Azure Policy. Azure Policy guarantees that resources adhere to business norms and legal requirements with a broad range of pre-built, customizable policy definitions. To provide a uniform and compliant environment, policy definitions specify the conditions to be met for resource attributes and the steps to be done when they are. The remediation task feature is very useful since it makes it possible to automatically fix resources that aren't compliant, protecting the Azure environment's security and integrity without requiring a lot of manual labor.

Additionally, the usage of resource locks adds a layer of protection against unintentional deletions and alterations post-deployment. Azure Policy serves as a governance tool before to deployment, whereas resource locks and role-based access control (RBAC) are post-deployment security controls. This all-encompassing strategy guarantees that resources are protected for the duration of their lives in addition to being consistent with defined standards from the beginning. In summary, the lab demonstrated how crucial it is to integrate these governance tools in order to create a reliable and secure Azure environment.