CANTON WEKE OTIENO

SECURITY ENGINEER TRACK

STUDENT TRACKING NUMBER; ADC-SE01-24010

CYBER SHUJAA

INSTRUCTOR: Dr. Paula

LAB 02B - MANAGE GOVERNANCE VIA AZURE POLICY

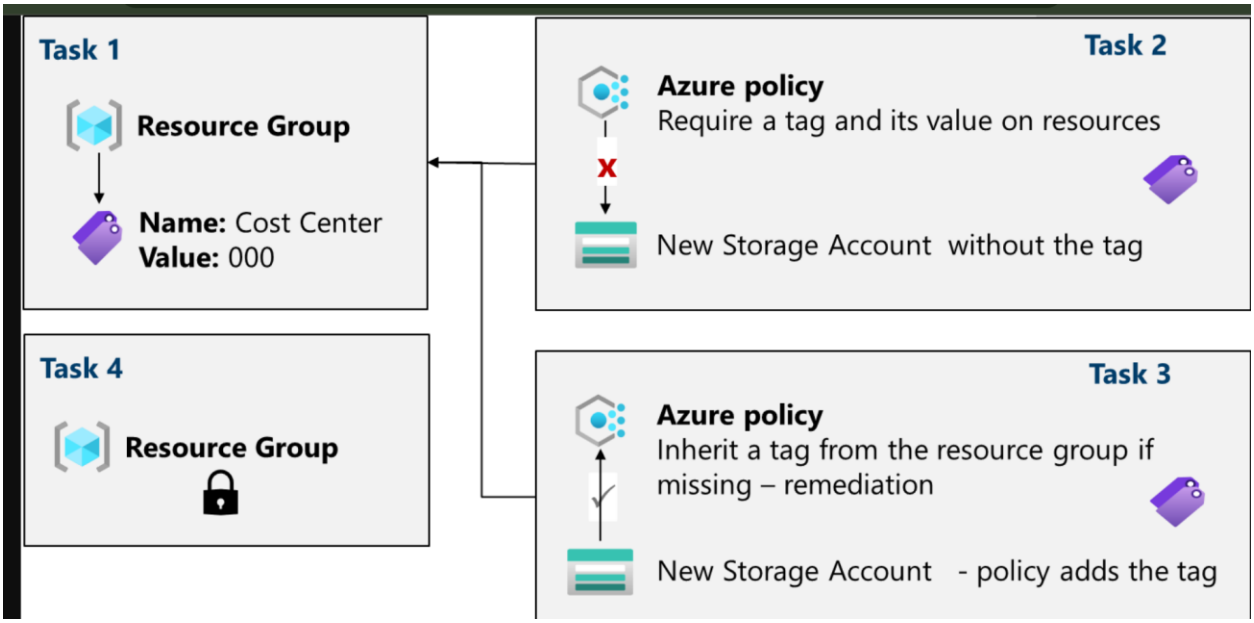
Introduction

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

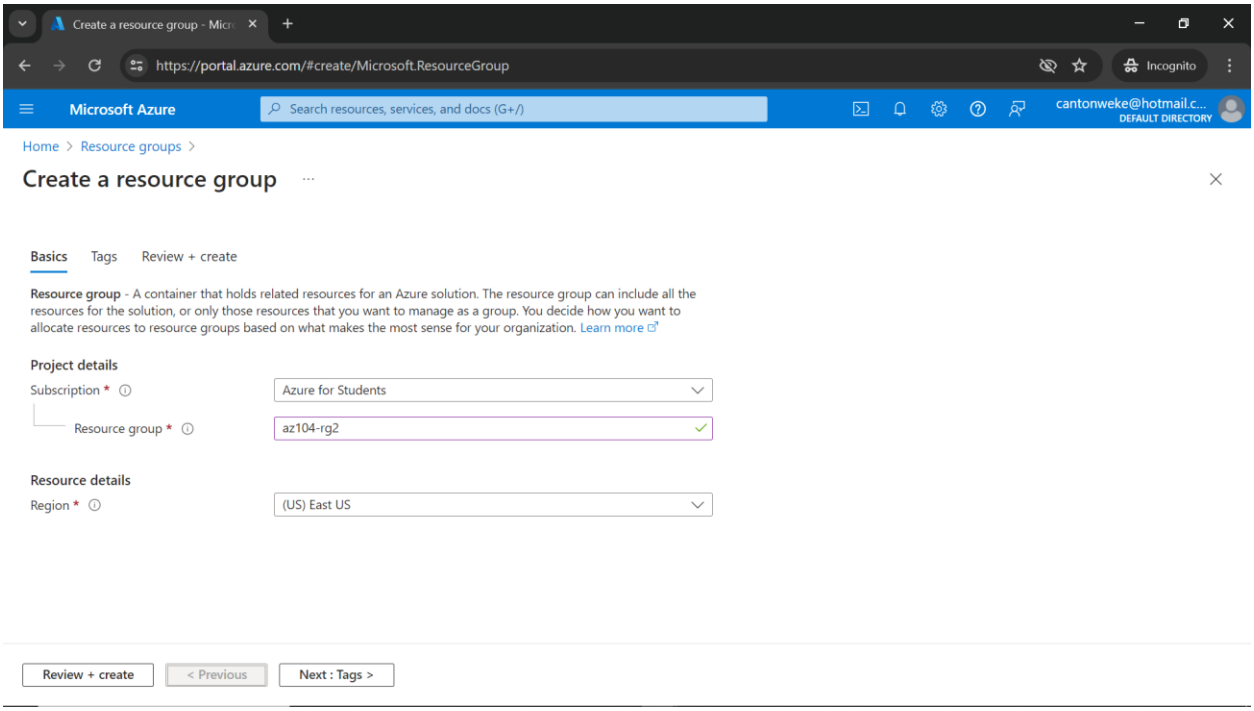
According to the Cloud Adoption Framework and Microsoft Well-Architected Framework, tags are an essential part of a governance approach. You may quickly find resource owners, sunset dates, group contacts, and other name/value pairs that are important to your company by using tags**.**

Instructions on how to create a resource group

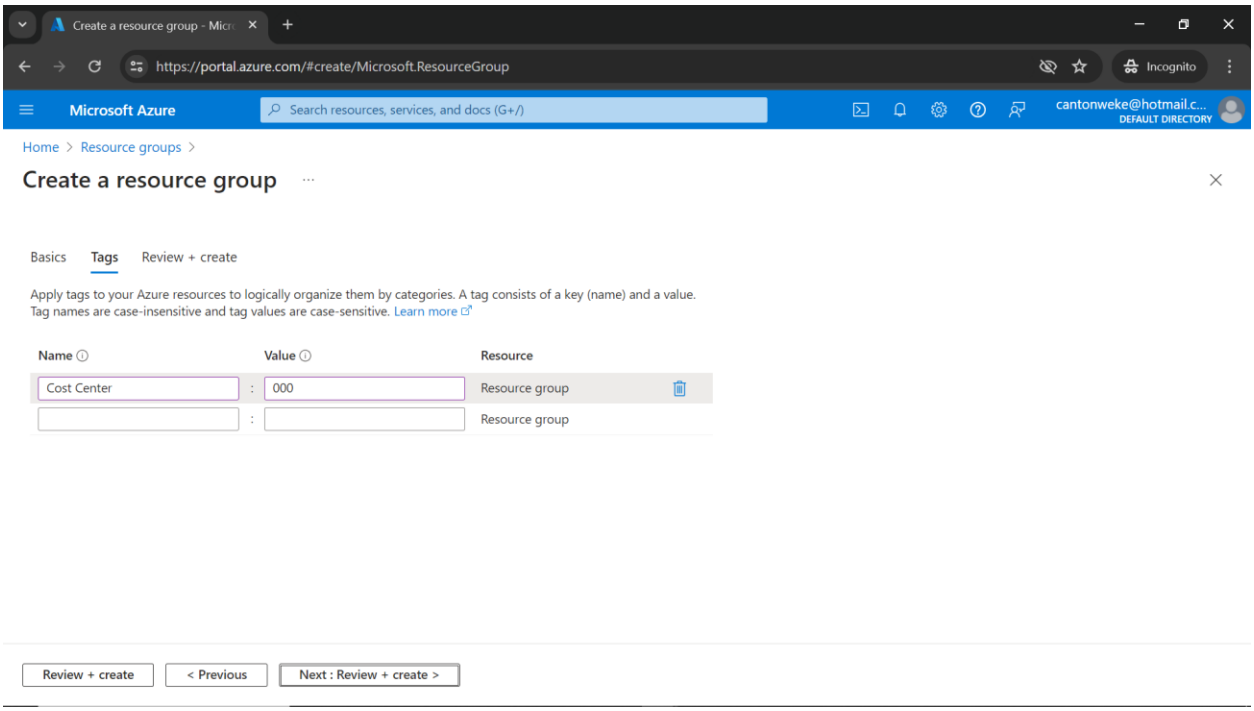
- Sign in to the Azure portal - https://portal.azure.com.
- Search for and select Resource groups.
- From the Resource groups, select + Create.
- Select Next: Tags and create a new tag.

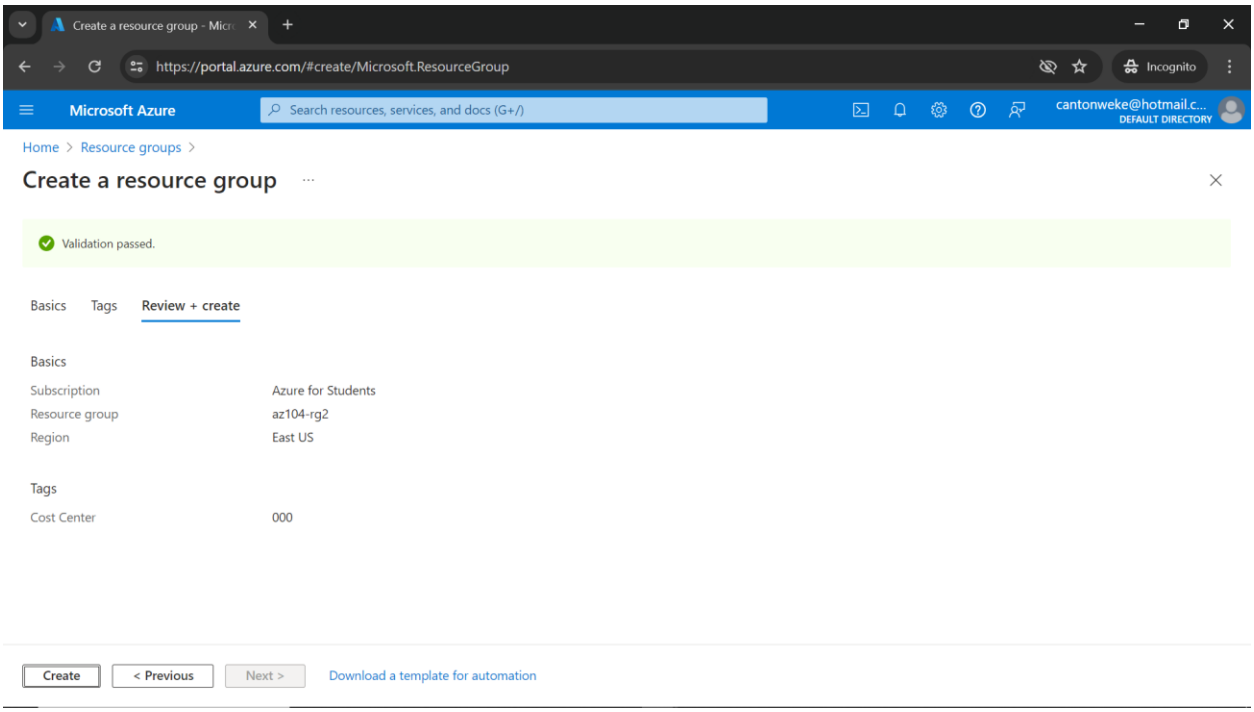
- Select Review + Create, and then select Create.

Screenshot showing how to create the resource groups

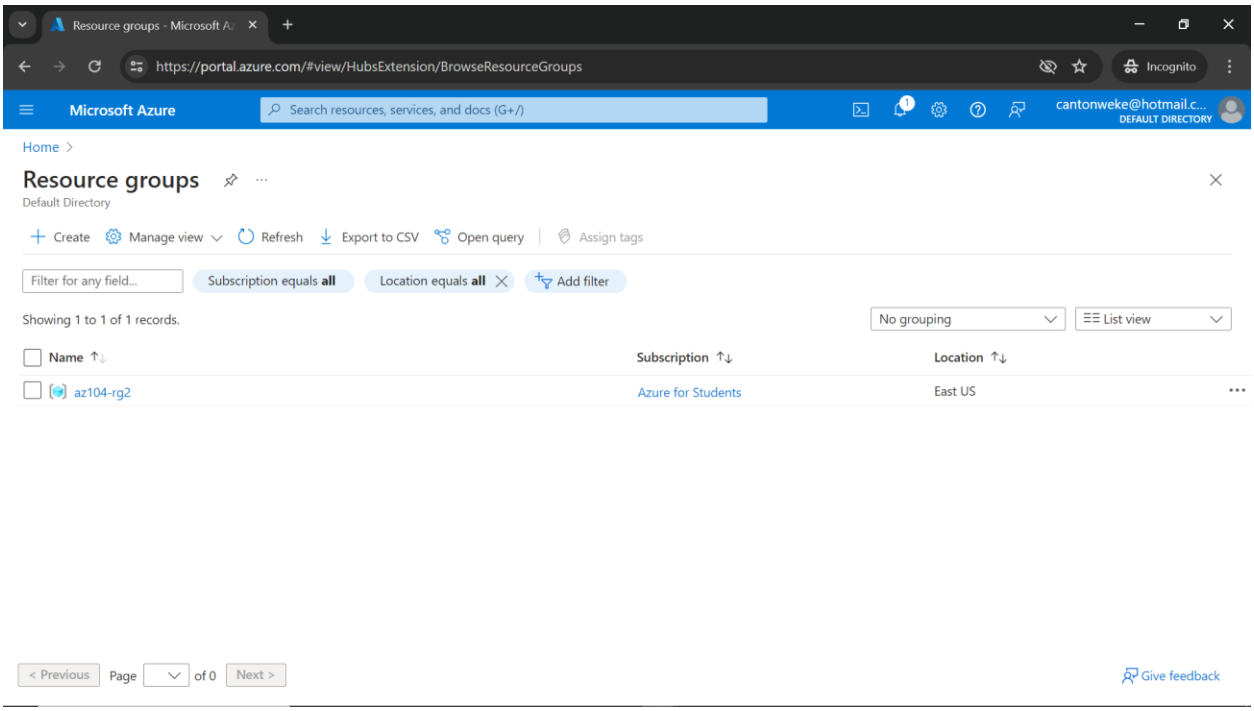


Tags



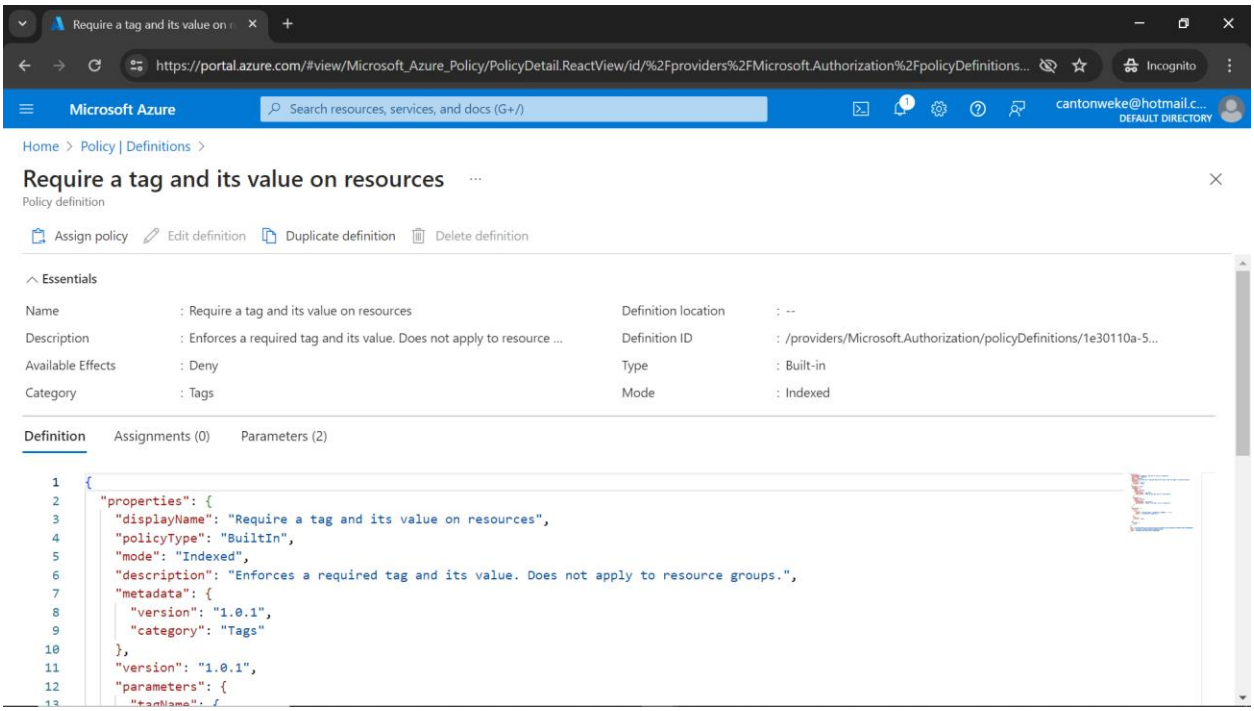


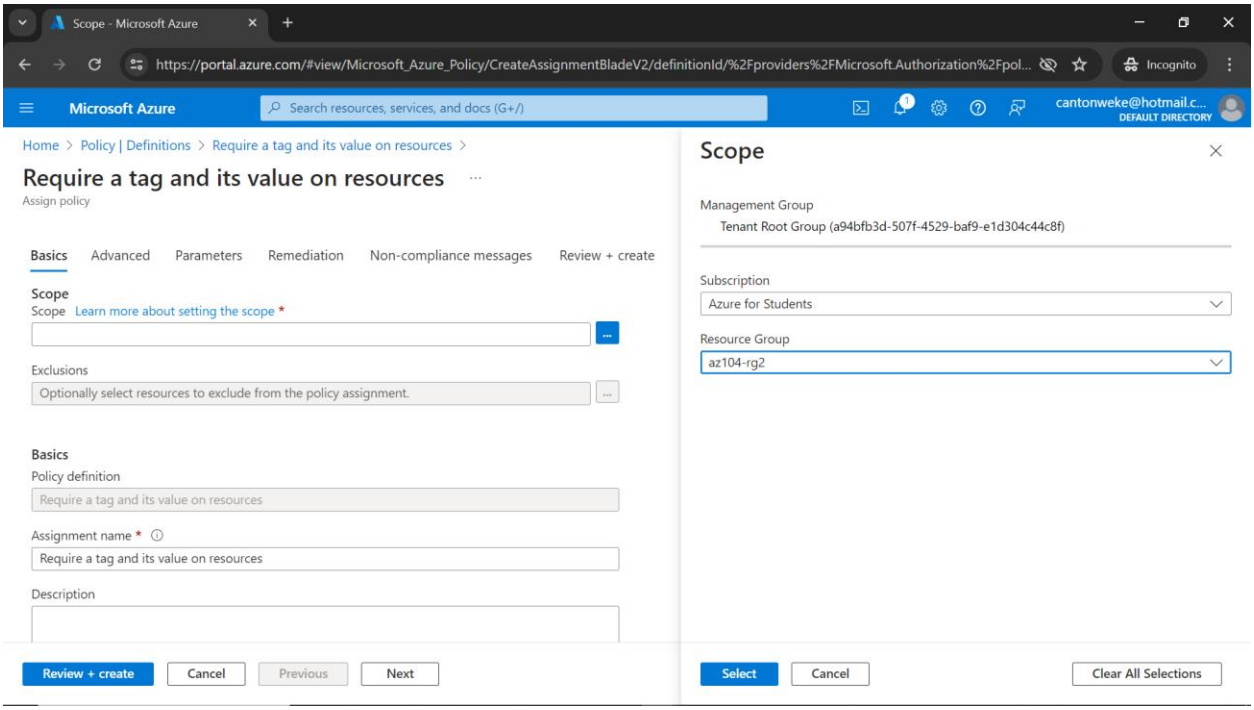
screenshot showing created Resource group



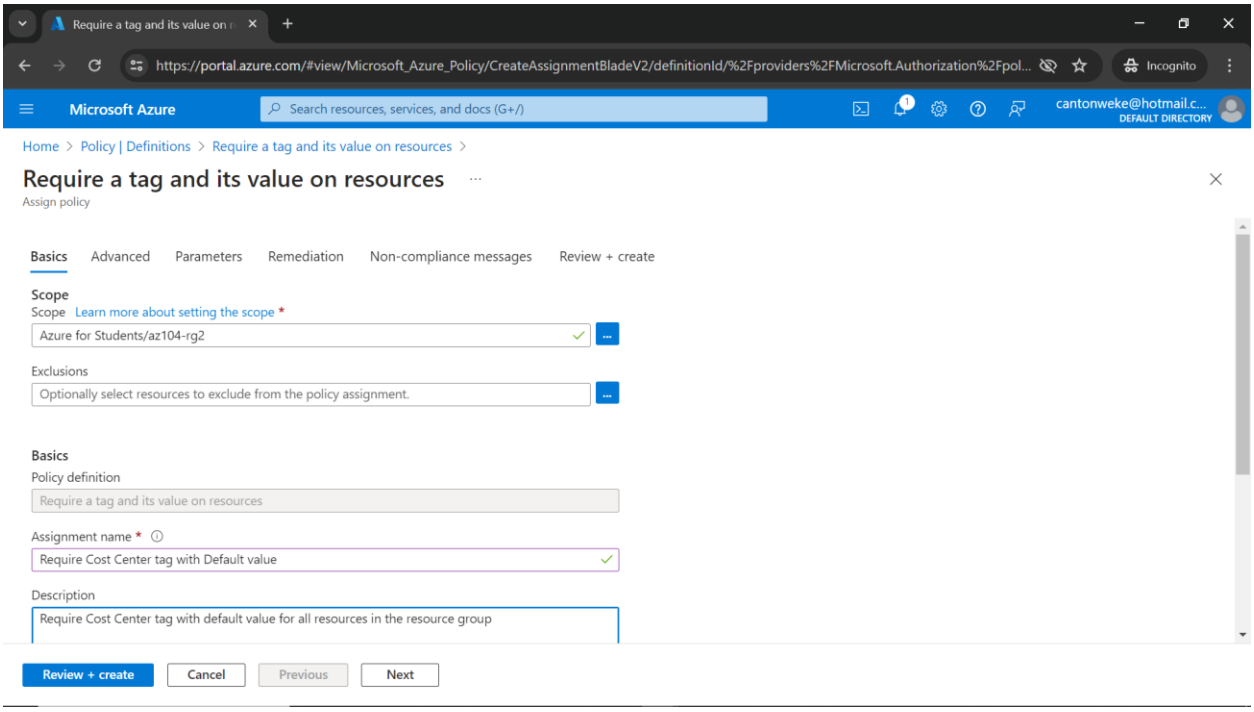
Task 2: Enforce tagging via an Azure Policy

Screenshot





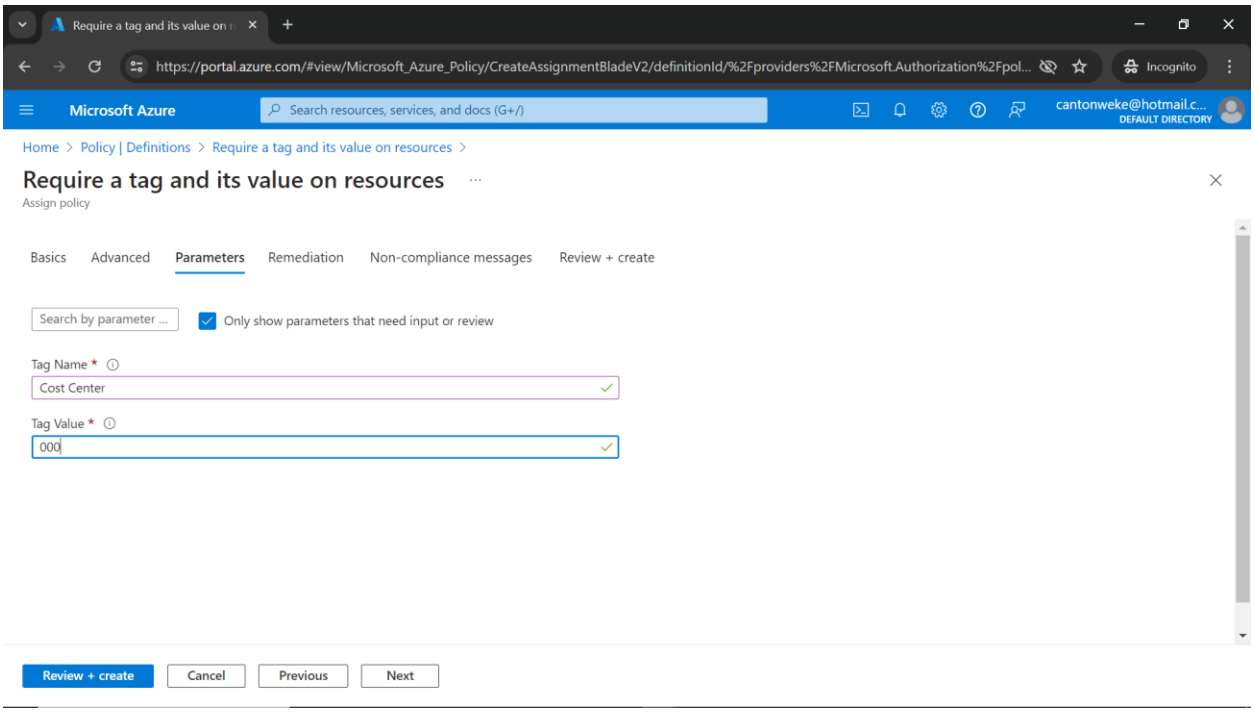
Configure the Basics properties of the assignment by specifying the following settings (leave others with their defaults): Screenshot



Click Next twice and set Parameters to the following values:

Setting	Value
Tag Name	Cost Center
Tag Value	000

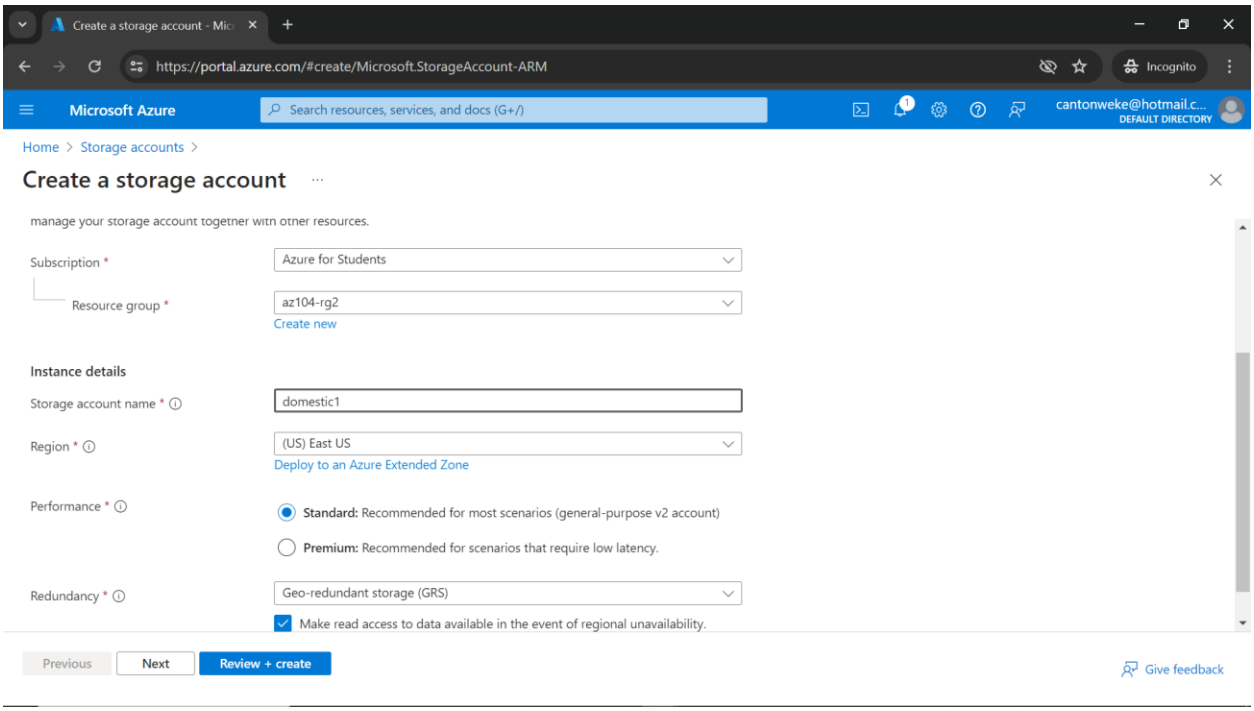
Screenshot



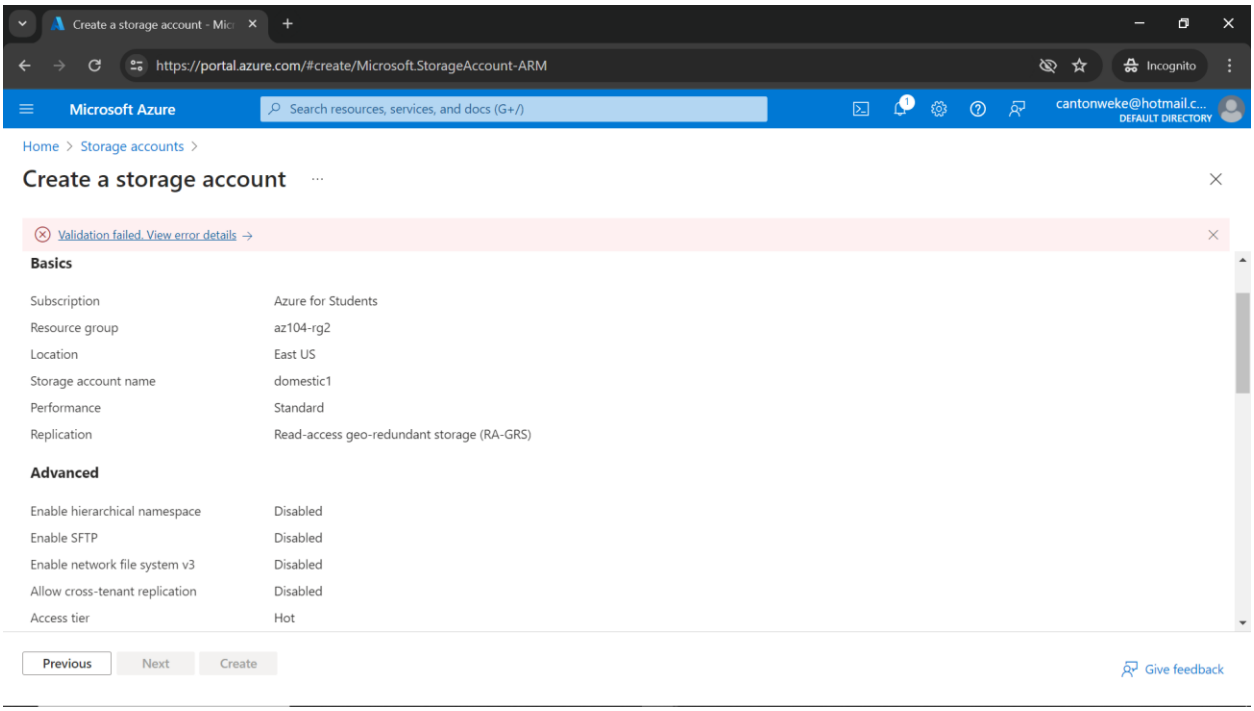
In the portal, search for and select Storage Account, and select + Create.

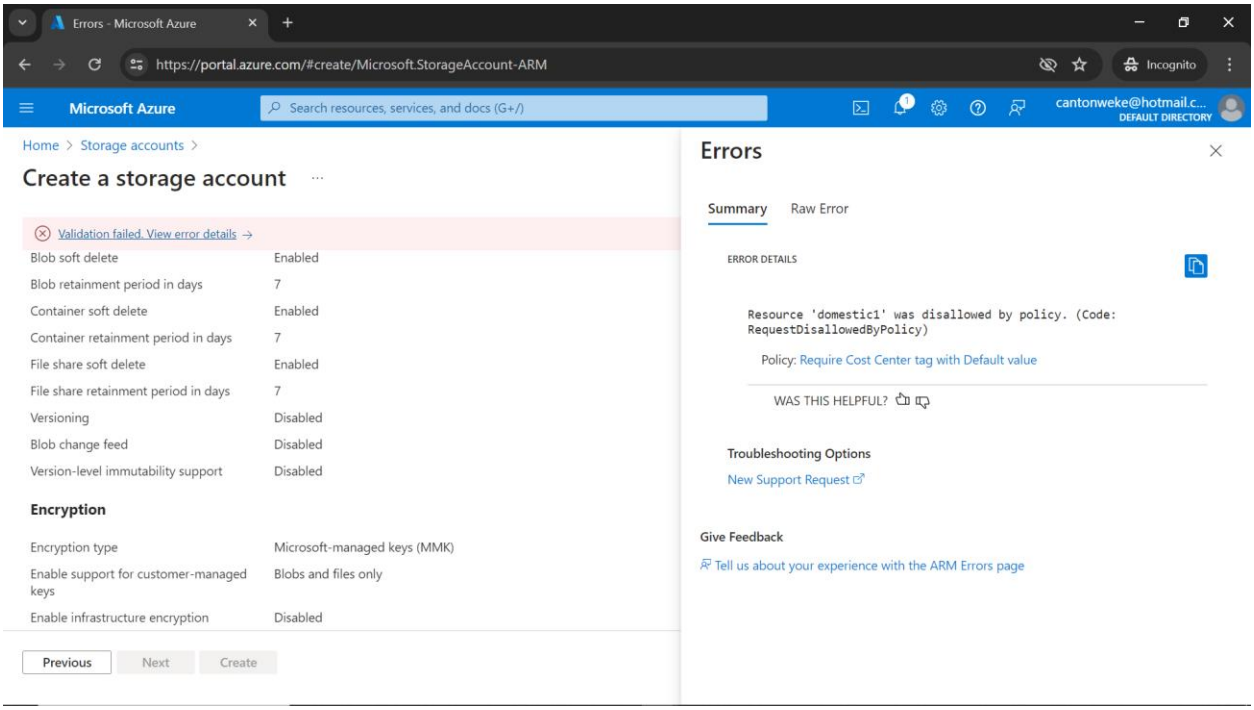
On the Basics tab of the Create storage account blade, complete the configuration.

Select Review and then click Create.



Screenshot showing validation error message.



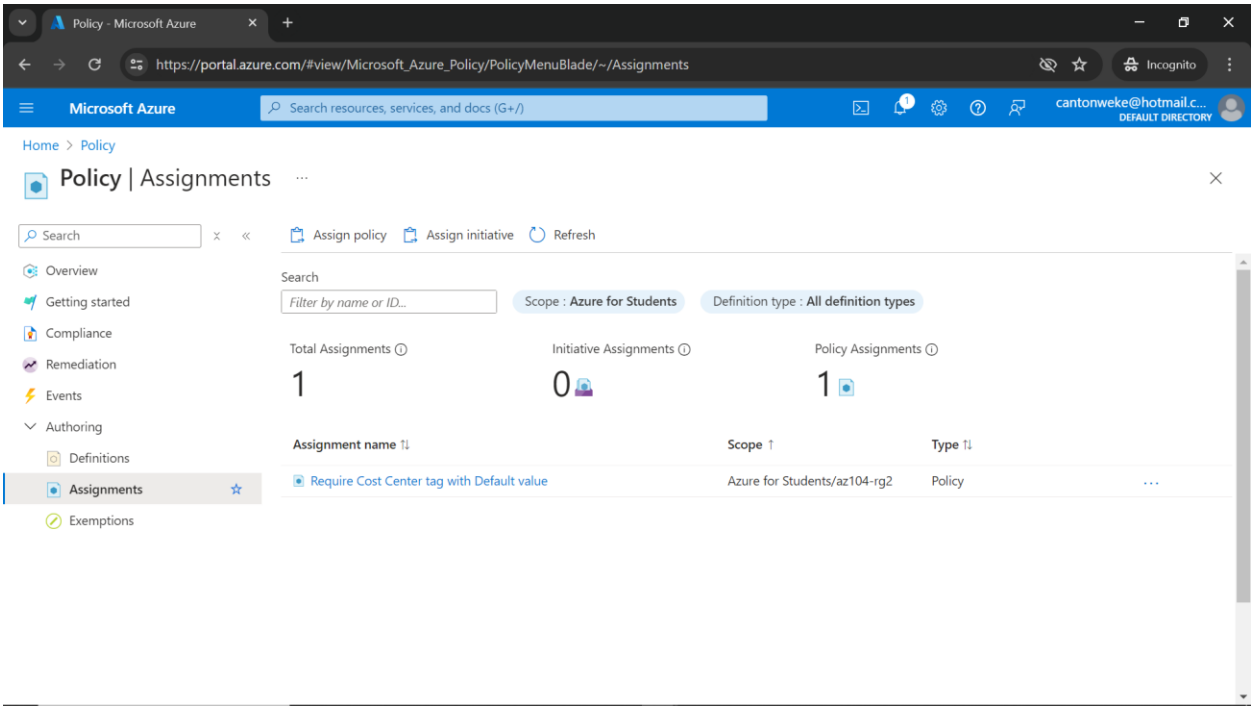


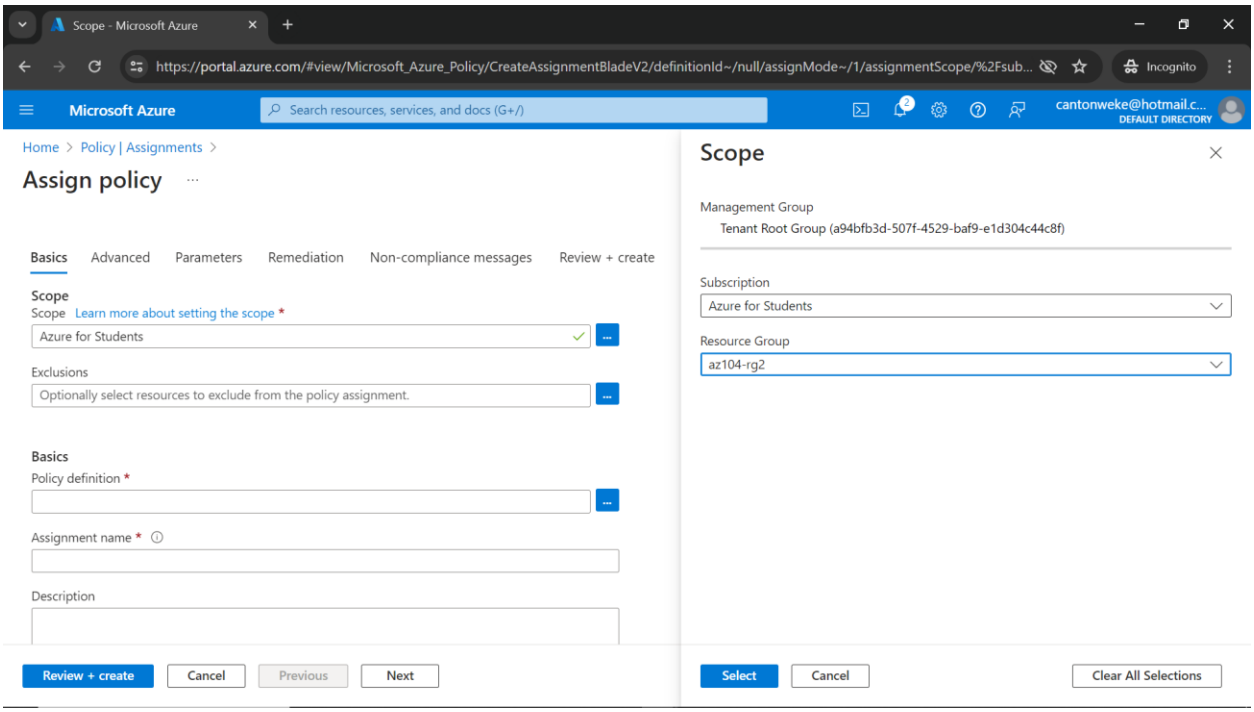
TASK 3: APPLY TAGGING VIA AN AZURE POLICY

Instructions and steps to complete the task.

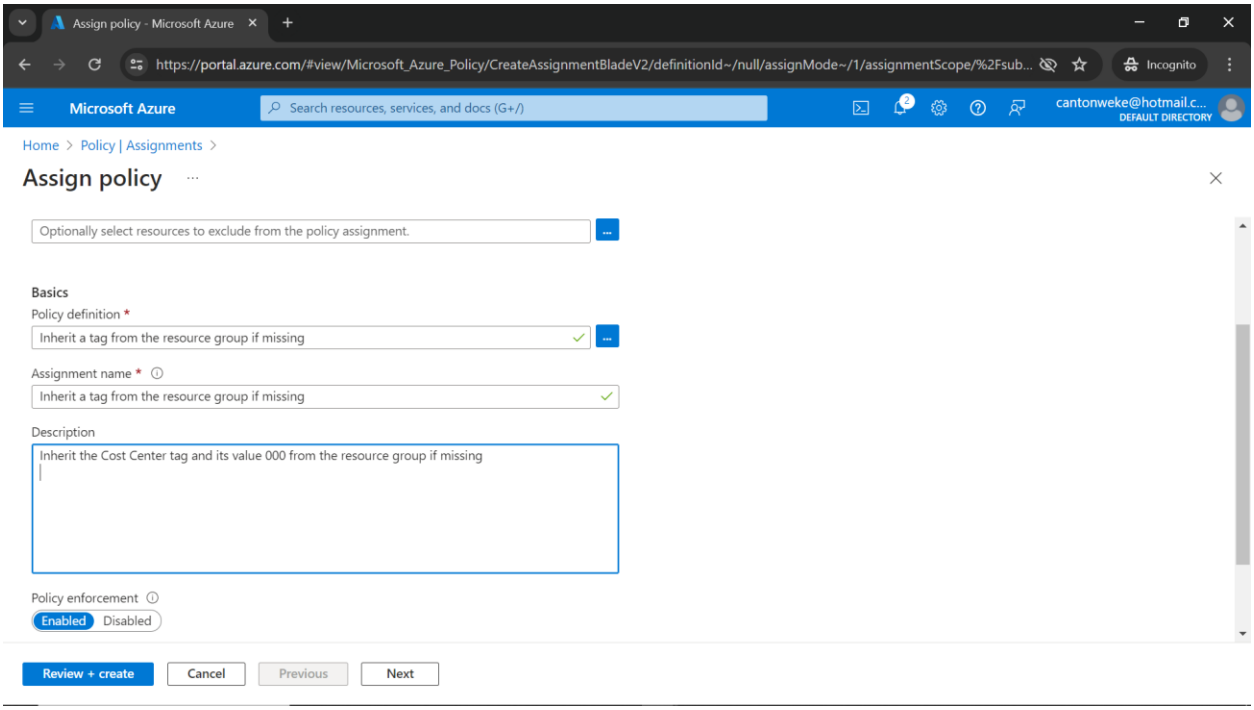
- In the Azure portal, search for and select Policy.
- In the Authoring section, click Assignments.
- In the list of assignments, click the ellipsis icon in the row representing the Require Cost Center tag with Default value policy assignment and use the Delete assignment menu item to delete the assignment.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

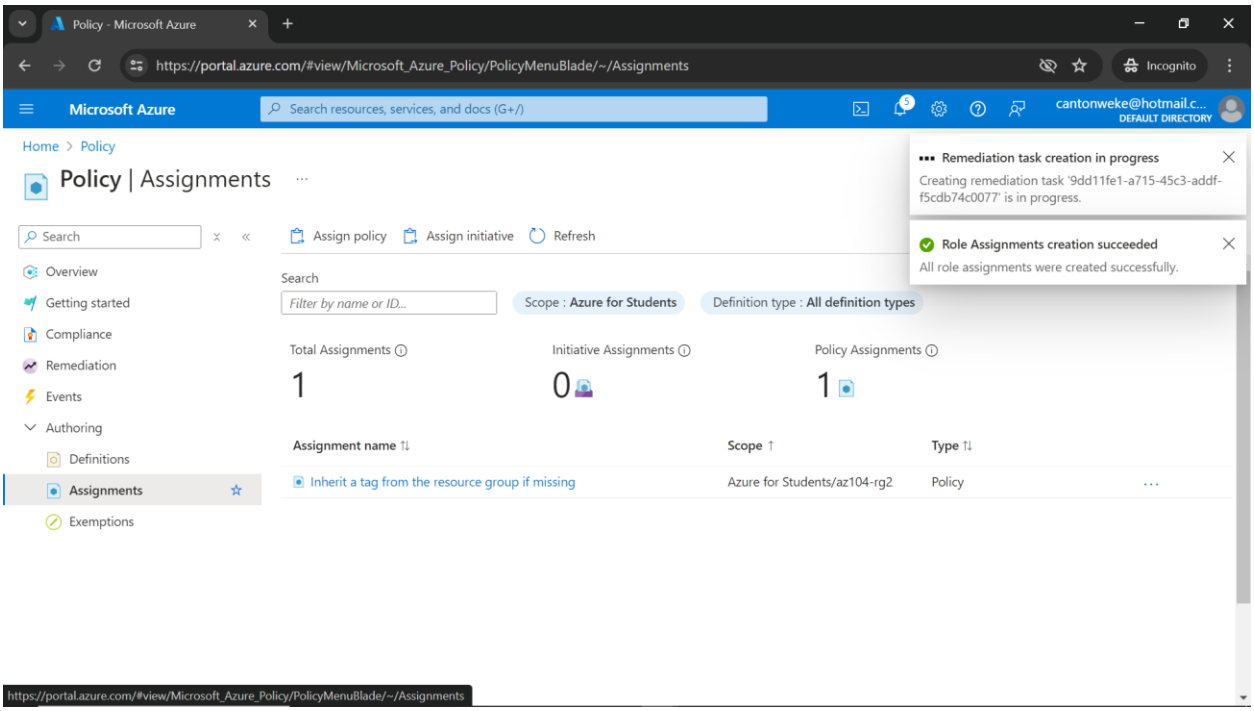
Screenshot


Policy - Microsoft Azure
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Assignments
Incognito
Microsoft Azure
Search resources, services, and docs (G+/)
cantonweke@hotmail.c...
DEFAULT DIRECTORY
Home > Policy
Policy | Assignments
Search
Overview
Getting started
Compliance
Remediation
Events
Authoring
Definitions
Assignments
Exemptions
Assign policy
Assign initiative
Refresh
Search
Filter by name or ID...
Scope : Azure for Students
Definition type : All definition types
Total Assignments
1
Initiative Assignments
0
Policy Assignments
1
Assignment name
Scope
Type
Require Cost Center tag with Default value
Azure for Students/az104-rg2
Policy


Scope - Microsoft Azure
https://portal.azure.com/#view/Microsoft_Azure_Policy/CreateAssignmentBladeV2/definitionId~/null/assignMode~/1/assignmentScope/%2Fsub...
Incognito
Microsoft Azure
Search resources, services, and docs (G+/)
cantonweke@hotmail.c...
DEFAULT DIRECTORY
Home > Policy | Assignments >
Assign policy
Basics
Advanced
Parameters
Remediation
Non-compliance messages
Review + create
Scope
Scope Learn more about setting the scope *
Azure for Students
Exclusions
Optionally select resources to exclude from the policy assignment.
Basics
Policy definition *
Assignment name *
Description
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

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

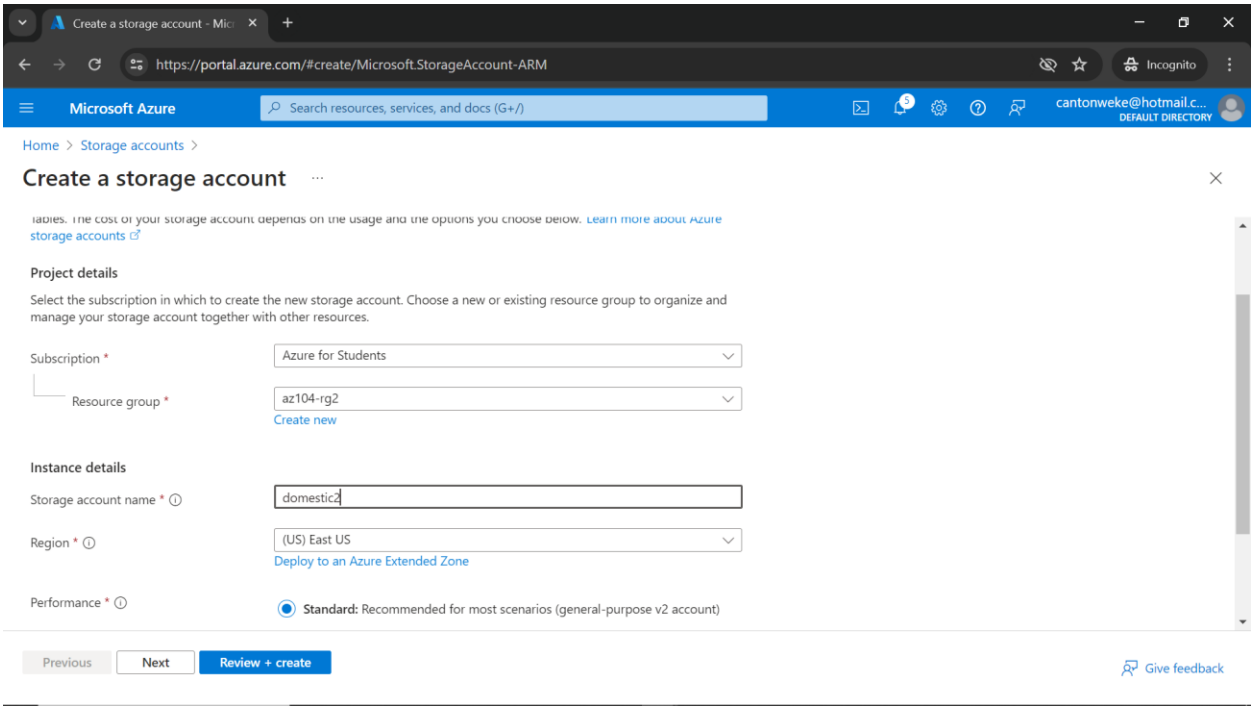




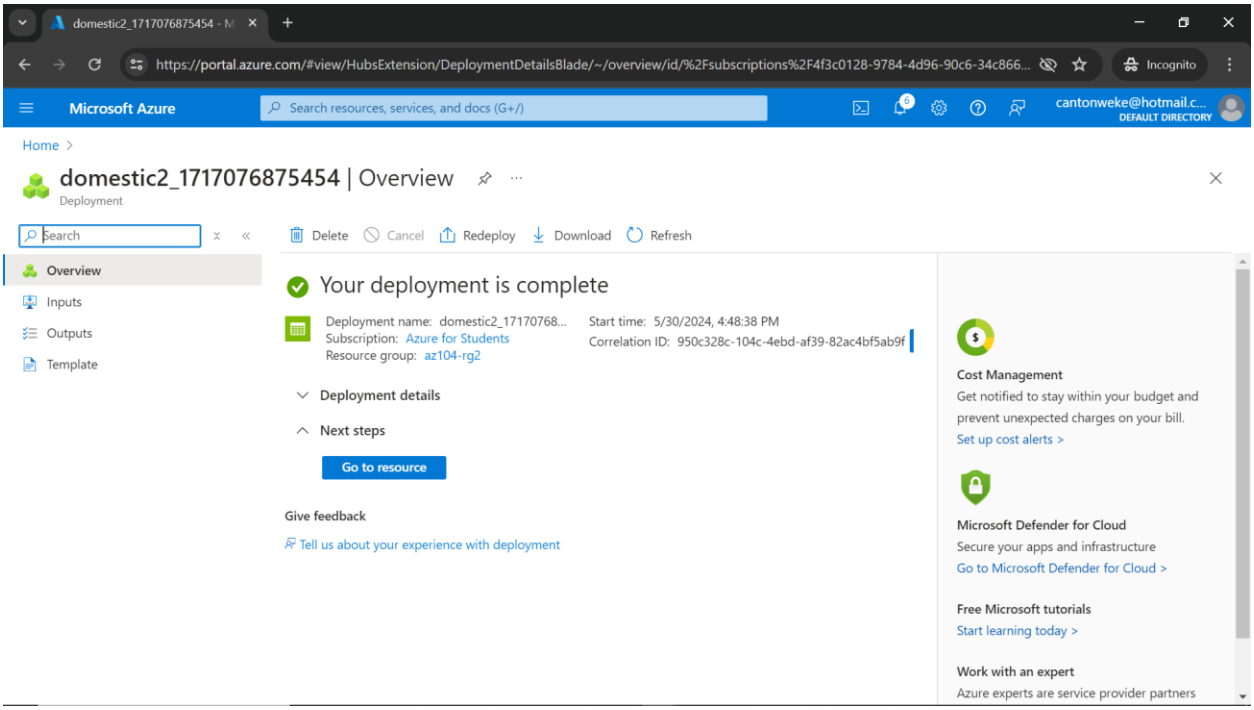
Search for and select Storage Account, and click + Create.

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



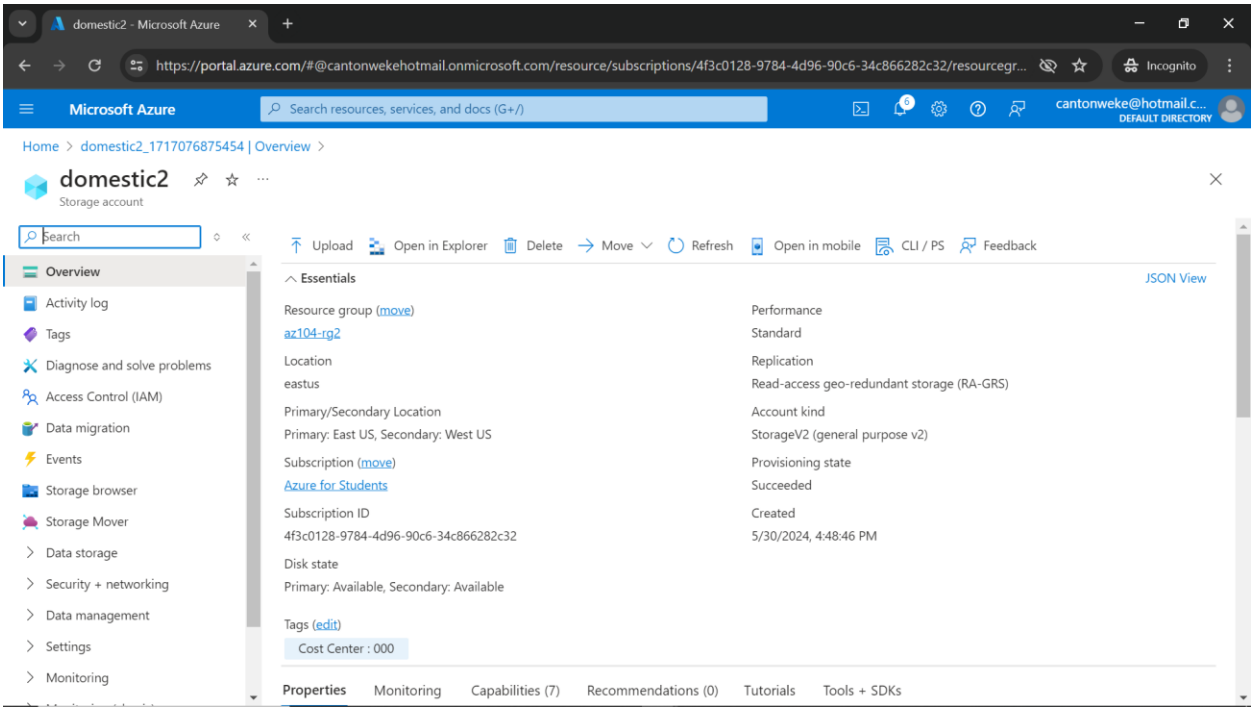
Screenshot showing created storage account



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



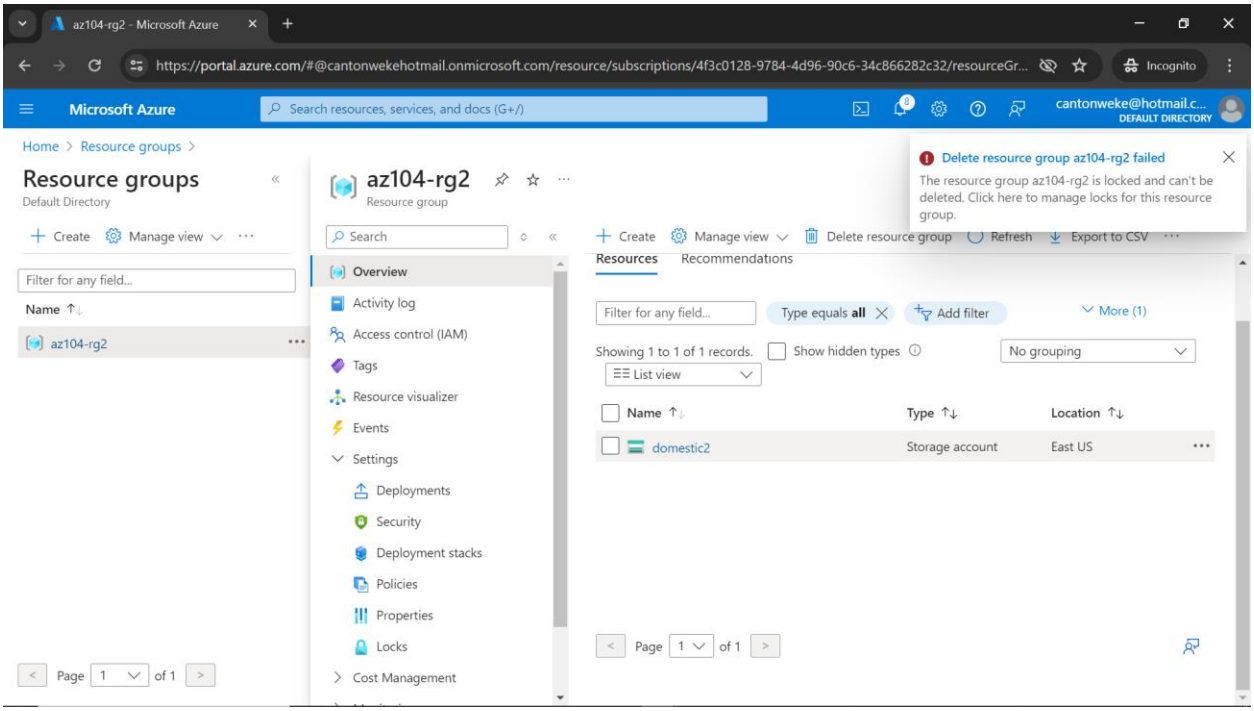
TASK 4: CONFIGURE AND TEST RESOURCE LOCKS

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.