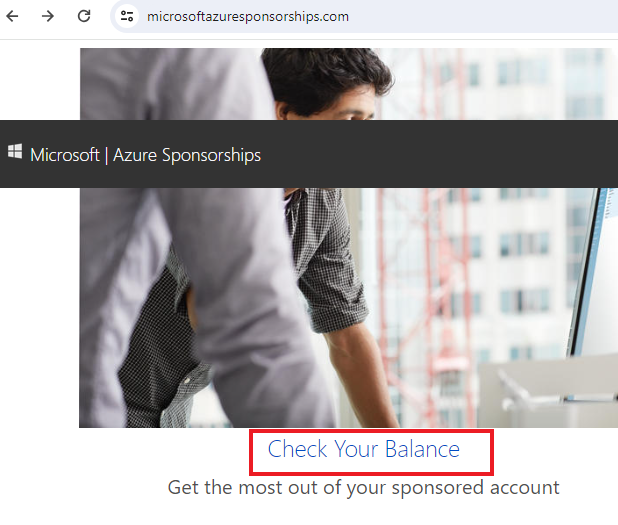


Lab 17: Create an Azure Policy

At the end of each lab, any resources you created in your account will be preserved. Some Azure resources, such as VM instances, may be automatically shut down, while other resources, such as storage services will be left running. Keep in mind that some Azure features cannot be stopped and can still incur charges (i.e. Azure Bastion). To minimize your costs, delete all resources and recreate them as needed to test your work during a session.

A screenshot of a computer

Description automatically generated with medium confidence



Reference: [AZ-900T0X-MICROSOFTAZUREFUNDAMENTALS](https://microsoftlearning.github.io/AZ-900T0x-MicrosoftAzureFundamentals)

# 17 - Create an Azure Policy

In this walkthrough, we will create an Azure Policy to restrict deployment of Azure resources to a specific location.

# Task 1: Create a resource group (5 min)

In this task, we will create a resource group for this exercise.

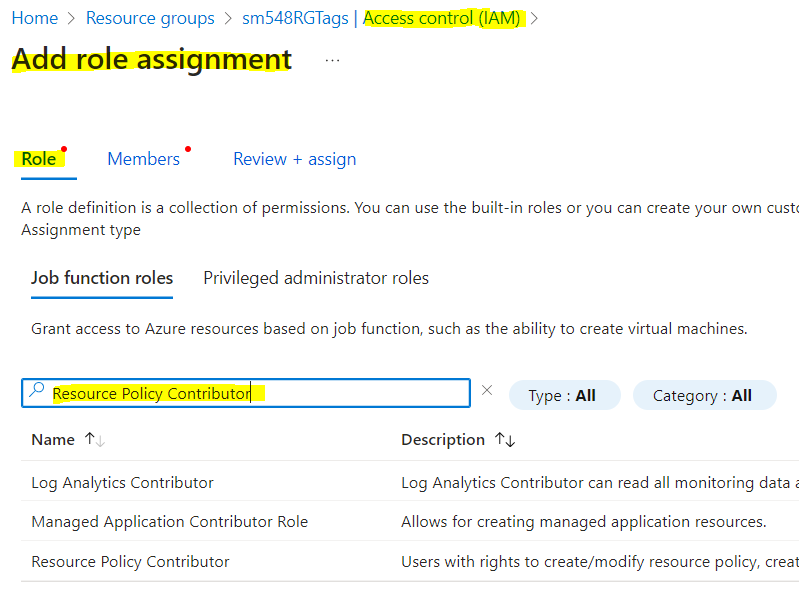
1. Sign in to the [Azure portal](https://portal.azure.com/) with with your **odl\_user\_xxx** azure account
2. From the **All services** blade, search for and select **Resource groups**, then select **+ Create**.
3. Create a new resource group. When you are done click **Review + create** and then **Create**.

| Setting | Value |
| --- | --- |
| Subscription | **Use your subscription (you should see “Seneca College : <course name>”)** |
| Name | **myRGTagPolicy** |
| Region | **(US) East US** |

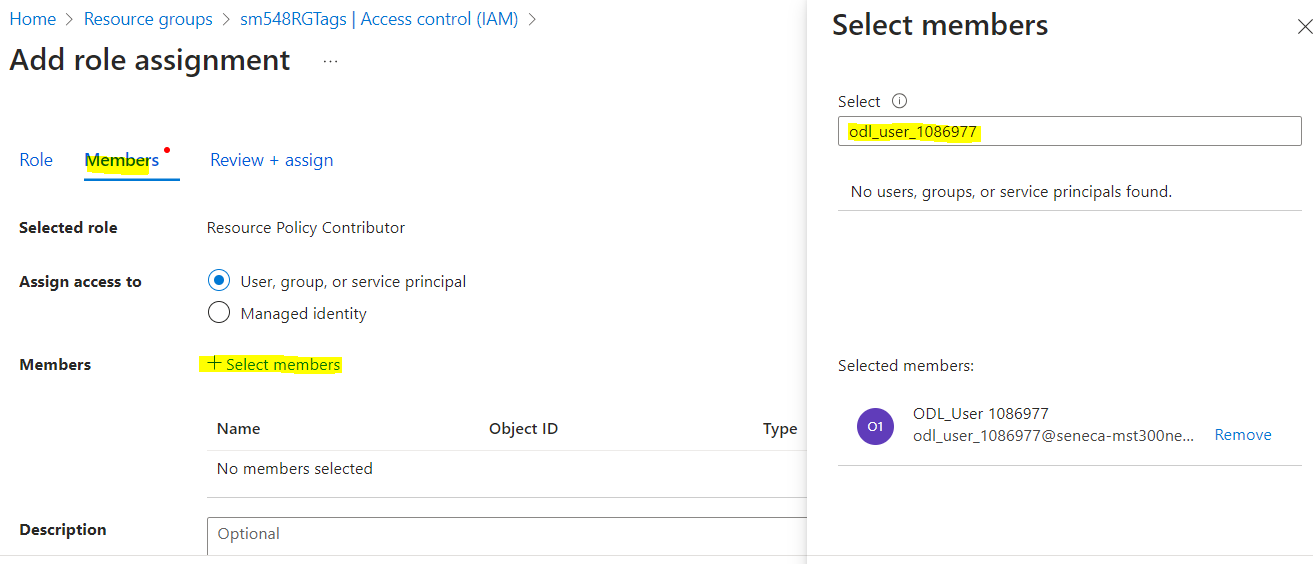
# Task 2: Assign the required permission of your CloudLab Account (5 min)

In this task, we will add the required permission to allow you to assign a policy to the new resource group.

1. Go to the Resource Group that you created in the above task and select **Access Control (IAM)**
2. From the **Access Control (IAM)**, select **Add** and **Add role assignment****,** search and selecr for **Resource Policy Contributor,** then click **Next**



1. Select the second tab (**Members**) and select “**+Select Member**”.
2. Search for **your** CloudLab account (ie. Odl\_user\_xxx@xxxxx)



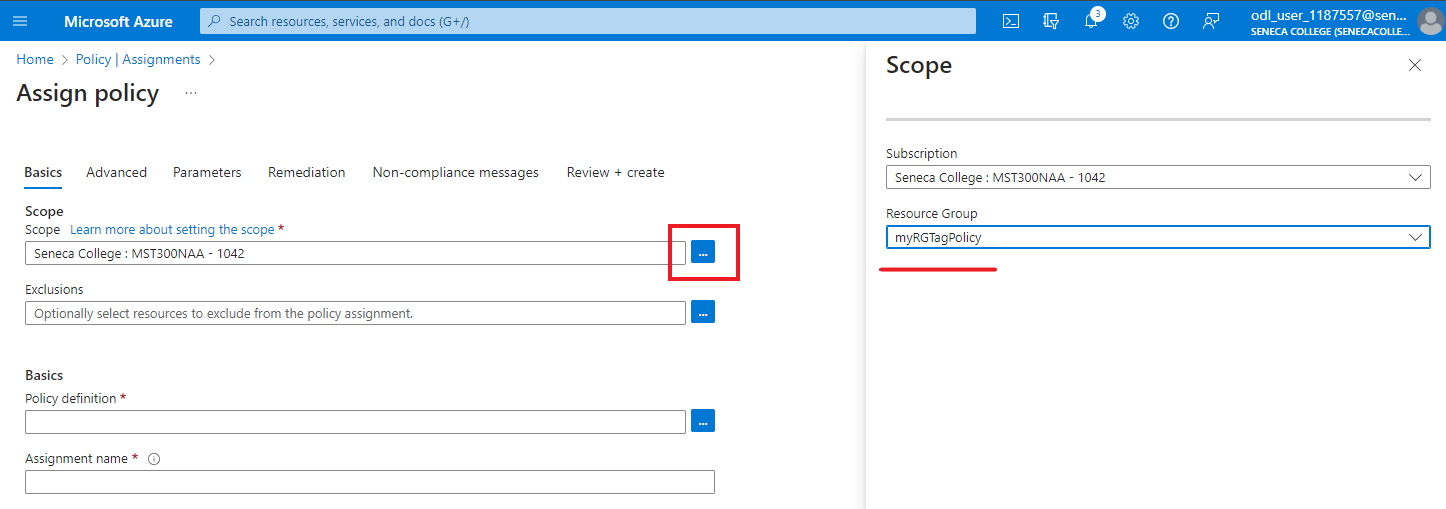
1. When you are done click **Review + assign**.
2. Now your CloudLab account has the required access to assign a policy to your new resource group from Task 1
3. Impotant: It may tae 5-10 min for the permission to be propely implemented.

# Task 3: Create a Policy assignment (10 min)

In this task, we will configure the allowed location policy and assign it to our subscription.

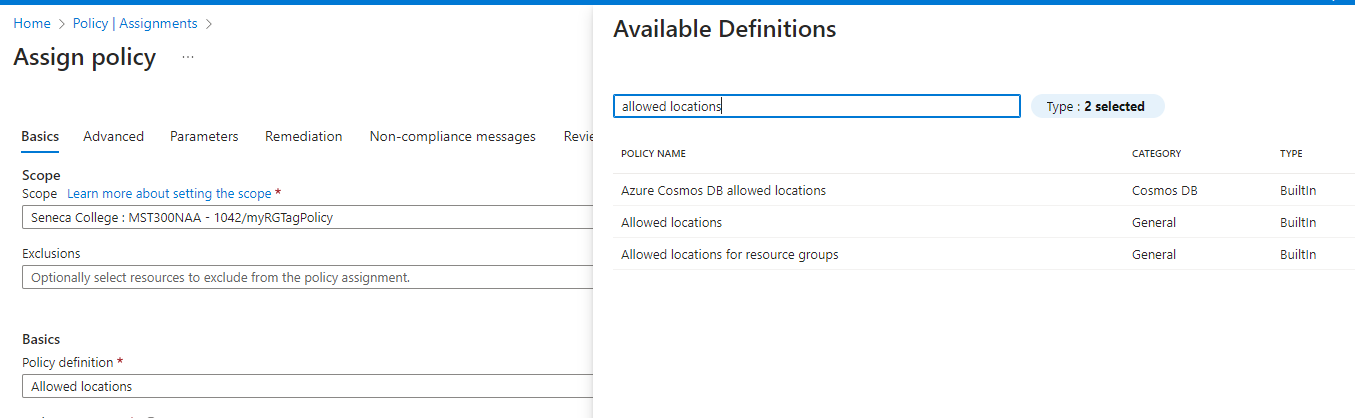
1. From the **All services** blade, search for and select **Policy**, under the **Authoring** section click **Definitions**. Take a moment to review the list of built-in policy definitions. For example, in the **Category** drop-down select only **Compute**. Notice the **Allowed virtual machine SKUs** definition enables you to specify a set of virtual machine SKUs that your organization can deploy.
2. Return to the **Policy** page, under the **Authoring** section click **Assignments**. An assignment is a policy that has been assigned to take place within a specific scope. For example, a definition could be assigned to the subscription scope.
3. Click **Assign Policy** at the top of the **Policy - Assignments** page.
4. On the **Assign Policy** page, select the Scope selector by clicking the ellipsis.
5. Ensure your subscription and new the resource group that you created in Task 1 is selected. Your subscription name might be different. Notice you can optionally scope the policy to a resource group. Leave the defaults and click **Select**.

**Note**: A scope determines what resources or grouping of resources the policy assignment applies to. In our case we could assign this policy to a specific resource group, however we chose to assign the policy at subscription level. Be aware that resources can be excluded based on the scope configuration. Exclusions are optional.

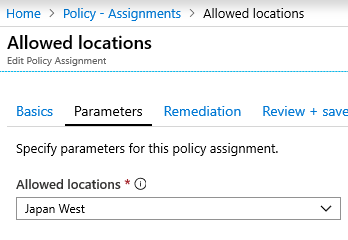


1. Select the **Policy definition** ellipsis button. In the **Search** box type **location** and click on the **Allowed locations** definition, then click **Add**.

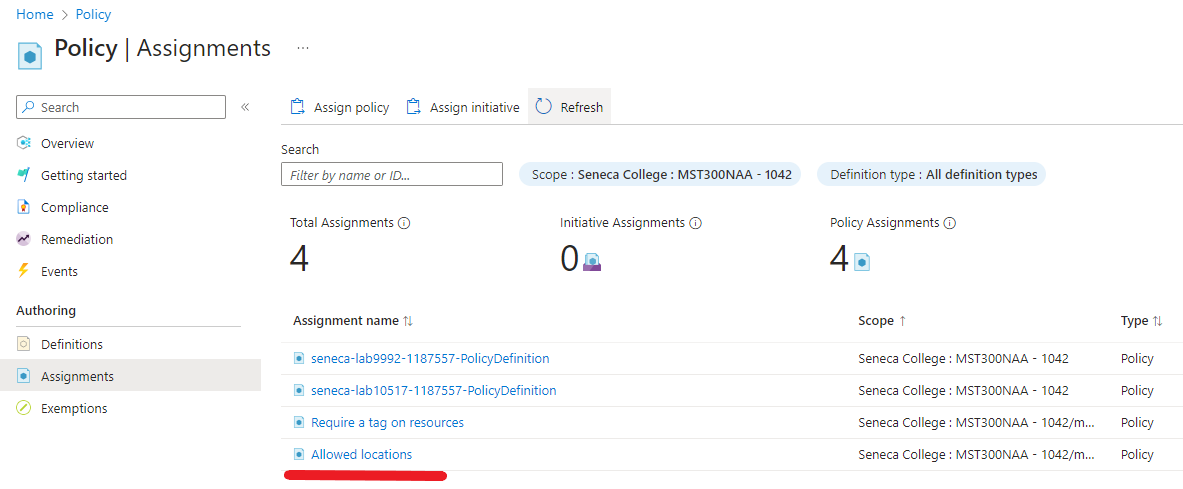
**Note**: This **Allowed Locations** policy definition will specify a location into which all resources must be deployed. If a different location is chosen, deployment will not be allowed. For more information view the [Azure Policy Samples](https://docs.microsoft.com/en-us/azure/governance/policy/samples/index) page.



1. In the **Assign policy** pane, switch to the **Parameters** tab, click on the arrow at the end of the **Allowed locations** box and from the subsequent list choose **Japan West**. Leave all other values as they are and click **Review + create**, and then **Create**.

[](https://microsoftlearning.github.io/AZ-900T0x-MicrosoftAzureFundamentals/Instructions/images/1404.png)

1. The **Allowed locations** policy assignment is now listed on the **Policy - Assignments** pane and it is now in place, enforcing the policy at the scope level we specified (subscription level).



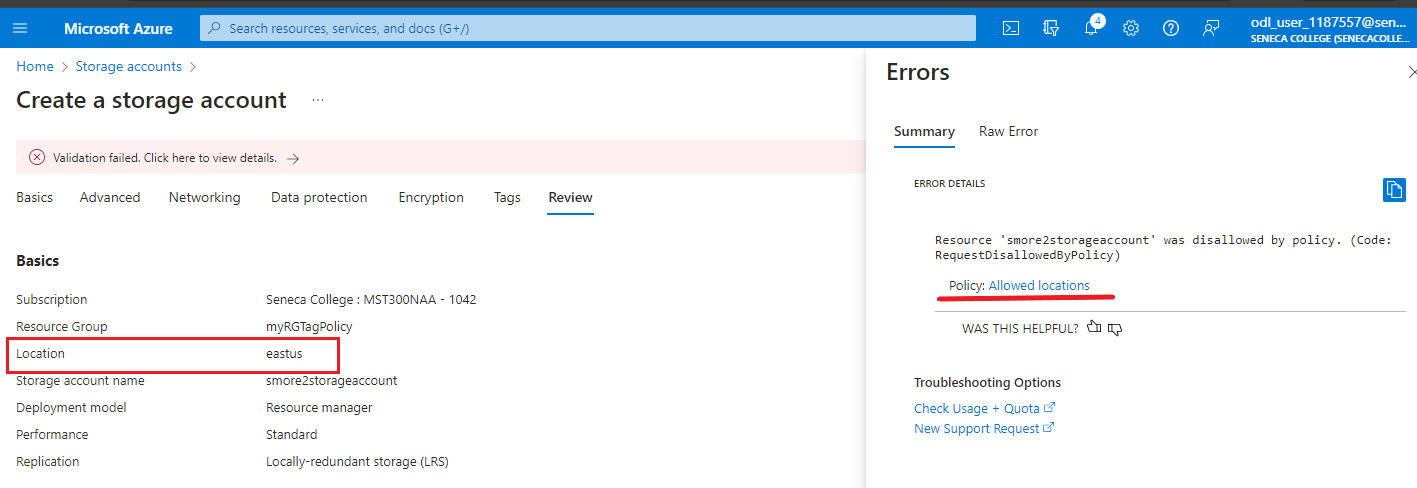
# Task 4: Test Allowed location policy

In this task, we will test the Allowed location policy.

1. In the Azure Portal, from the **All services** blade, search for and select **Storage accounts**, and then click **+ Create**.
2. Configure the storage account (replace **xxxx** in the name of the storage account with letters and digits such that the name is globally unique). Leave the defaults for everything else.

| Setting | Value |
| --- | --- |
| Subscription | **Use your subscription** |
| Resource group | **myRGTagPolicy** |
| Storage account name | **<studentID>storageaccountxxxx (example: smore2storageaccount)** |
| Location | **(US) East US** |
| Redundacy | **Locally-redundantstorage (LRS)** |

1. Click **Review + create** and then click **Create**.
2. You will receive the deployment failed error stating that resource was disallowed by policy, including the **Allowed locations** policy name.



# Task 5: Delete the policy assignment

In this task, we will remove the Allowed location policy assignment and test.

We will delete the policy assignment to ensure we are not blocked on any future work we wish to do.

1. From the **All services** blade, search for and select **Policy**, and then click in the 3 dots next to the **Allowed locations** policy; and click in **Delete Assignment**
2. Confirm you wish to delete the policy assignment in the **Delete assignment** dialogue by clicking **Yes**
3. Try to create another storage account to ensure the policy is no longer in effect.

**Note**: Common scenarios where the **Allowed locations** policy can be useful include:

* + Cost Tracking: You could have different subscriptions for different regional locations. The policy will ensure that all resources are deployed in the intended region to help cost tracking.
  + Data Residency and Security compliance: You could also have data residency requirements, and create subscriptions per customer or specific workloads, and define that all resources must be deployed in a particular datacenter to ensure data and security compliance requirements.

Congratulations! You have created an Azure Policy to restrict deployment of Azure resources to a particular datacenter.

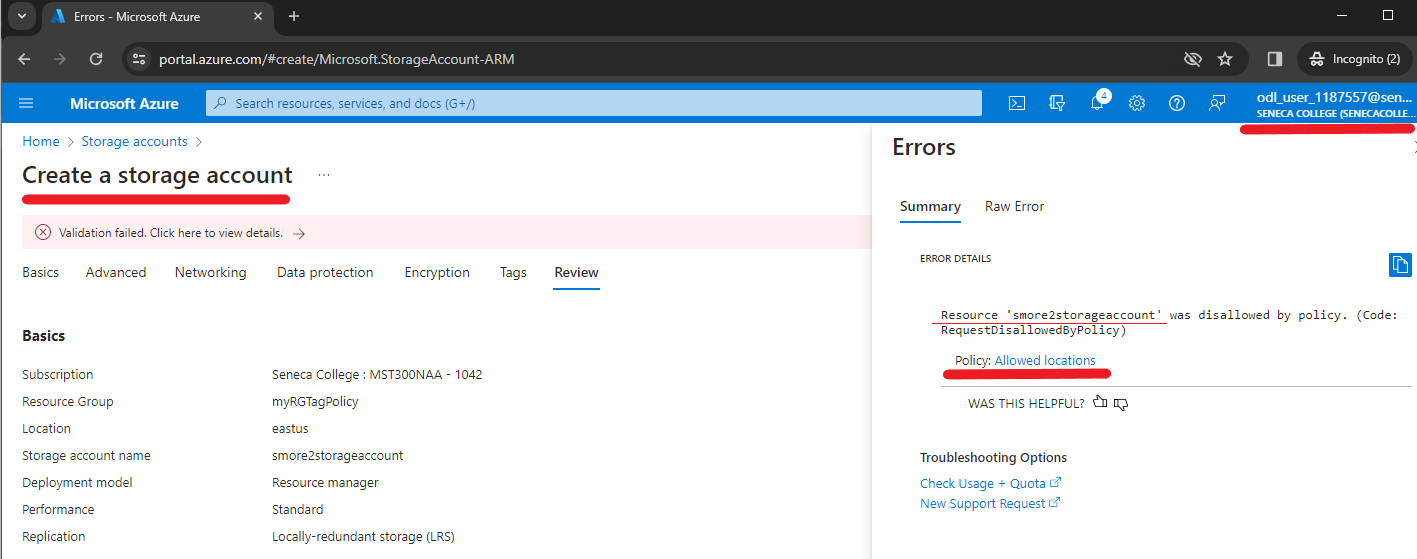
**Note**: To avoid additional costs, you can remove all resources in the resource group. Search for resource groups, click your resource group, and then delete the resources within the resource group. **DO NOT DELETE YOUR RESOURCE GROUP.**

# Submission Requirements

Submit a screenshot with the following information:

**Screenshot #1:**

* Error message when attempting to create a storage account in the incorrect location
* Error details displaying the policy being applied
* The Azure Portal with your **CloudLab Account** [requires another browser window]
  + **Note**: underline the above items as described in the below picture



**Screenshot #2:**

* Successful deletion of all resources within resource group. **DO NOT DELETE YOUR RESOURCE GROUP!**
  + To delete all resources with a resource group, go to “**Resource Group**”, select “**myRGTagPolicy**”, select all resources within the resource group, and select “**Delete**”

