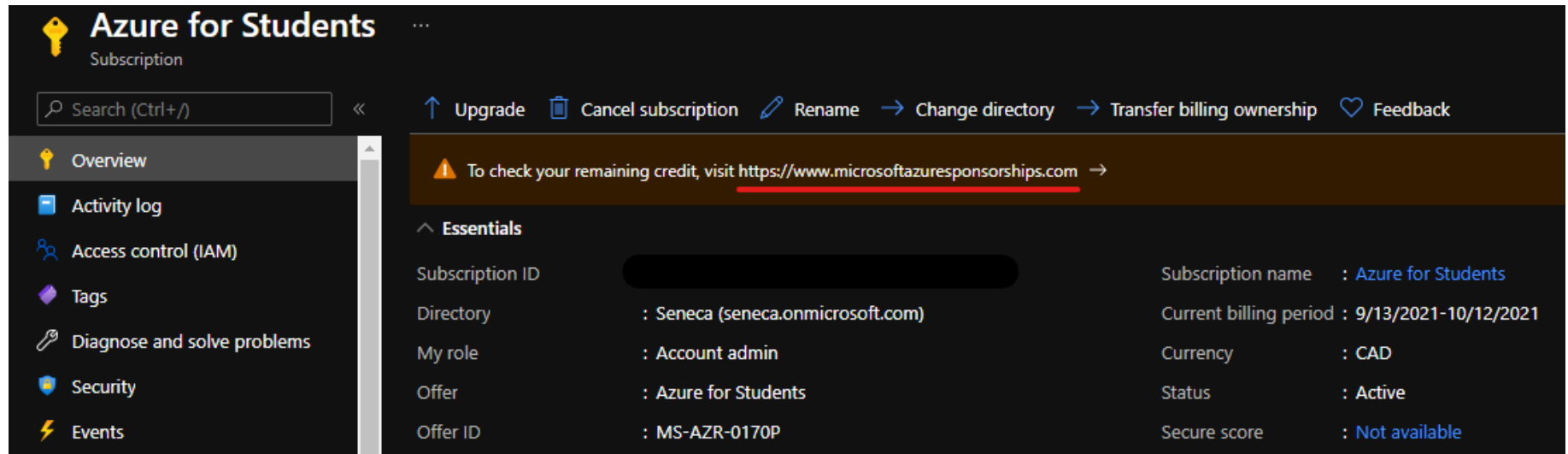# Seneca

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.

Reference: 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 Policy assignment (10 min)

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

1. Sign in to the Azure portal.
2. 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.
3. 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.
4. Click **Assign Policy** at the top of the **Policy - Assignments** page.
5. On the **Assign Policy** page, select the Scope selector by clicking the ellipsis.

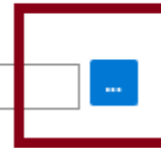6. Ensure your subscription is selected. Your subscription name might be different. Notice you can optionally scope the policy to a resource group. Leave the defaults and click **Select**.

   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.

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

    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](#) page.

Available Definitions   ✕

Type   Search
[All types   ∨]   [location   ]

Policy Definitions (3)
_____

Audit resource location matches resource group location

Built-in

Audit that the resource location matches its resource group location

Allowed locations

Built-in

This policy enables you to restrict the locations your organization can specify when deploying resources. Use to enforce your geo-compliance requirements. Excludes resource groups, Microsoft.AzureActiveDirectory/b2cDirectories, and resources that use the 'global' region.

Allowed locations for resource groups
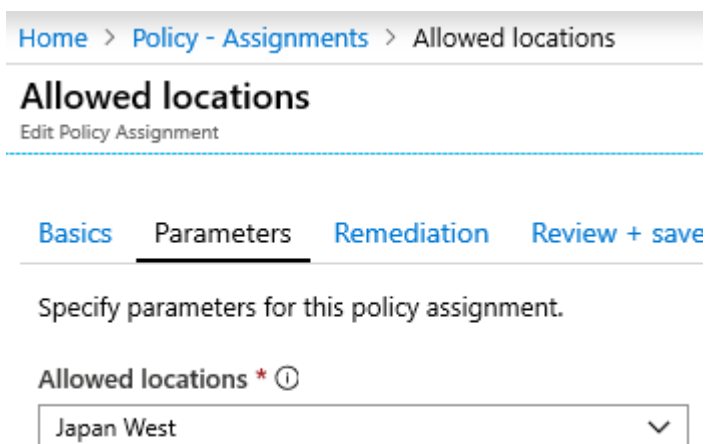
Built-in

This policy enables you to restrict the locations your organization can create resource groups in. Use to enforce your geo-compliance requirements.

[Select]   [Cancel]

8. 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**.

Home > Policy - Assignments > Allowed locations

Allowed locations
Edit Policy Assignment

Basics   **Parameters**   Remediation   Review + save

Specify parameters for this policy assignment.

Allowed locations * ⓘ

| Japan West | ⌄ |

9. 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 2: 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 **+ Add**.
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	**myRGPolicy** (create new)
Storage account name	**<studentID>storageaccountxxxx (example: dtrinh1storageaccount)**
Location	**(US) East US**

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

Task 3: 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 your **Allowed locations** policy.

   Note: On the **Policy** blade, you can view the compliance state of the various policies you have assigned.

   Note: The Allowed location policy may show non-compliant resources. If so, these are resources created prior to the policy assignment.

2. Click **Delete Assignment** in the top menu.

Home > Policy > Allowed locations

Allowed locations
Policy compliance

🔲 View definition   ✏️ Edit assignment   🗑️ Delete assignment   〽️ Create Remediation Task

Compliance state ⓘ	Overall resource compliance ⓘ	Non-compliant resources ⓘ
❌	0%	26 ◈
Non-compliant	0 out of 26	out of 26

◈ srv-jump	resourcegroups/myrgfw	⊗ Non-compliant
◈ srv-work	resourcegroups/myrgfw	⊗ Non-compliant
◈ mypsvm	resourcegroups/mypsvm	⊗ Non-compliant
◈ akvtest113	resourcegroups/myrgkv	⊗ Non-compliant
◈ test-fw-vn	resourcegroups/myrgfw	⊗ Non-compliant
◈ cs4aa509d922cc7x4eb9x9ae	resourcegroups/cloud-shell-storage-westus	⊗ Non-compliant

3. Confirm you wish to delete the policy assignment in the **Delete assignment** dialogue by clicking **Yes**
4. 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:

   o *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.

- o *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 login ID
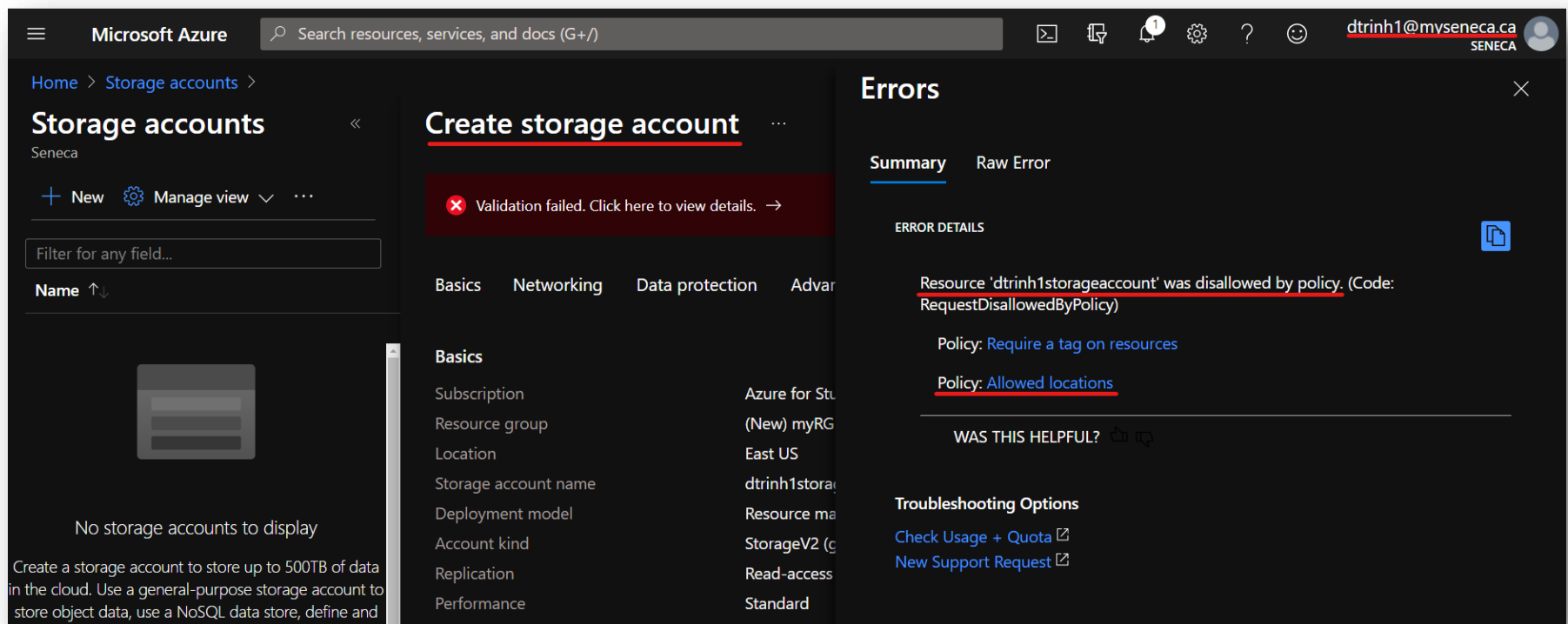
Screenshot #2:

- Successful deletion of resources within resource group. **DO NOT DELETE YOUR RESOURCE GROUP!**