

Yumaan Mustafa

BSSE 7A

2280133

Lab 10

10 - Create an Azure Policy (10 min)

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

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

1. Sign in to the Azure portal.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with icons for 'Create a resource', 'Policy', 'Resource groups', 'Storage accounts', 'Virtual machines', 'Virtual networks', 'Key vaults', 'App Services', 'Quickstart Center', and 'More services'. Below this is a search bar and a user profile icon. The main content area is titled 'Azure services' and 'Resources'. Under 'Recent', there are three items listed: 'Lab9' (Resource group), 'storageaccount331' (Storage account), and 'Azure subscription 1' (Subscription). A 'See all' link is at the bottom of this list. At the bottom of the page, there are sections for 'Navigate' (Subscriptions, Resource groups, All resources, Dashboard) and 'Tools'.

2. From the All services blade, search for and select Policy, under the Authoring section click Definitions.

All services

All



policy



Service providers : All

Release Status



Policy



Web Application Firewall policies (WAF)



Application security groups

Keywords: Policy, Policies



Bastions

Keywords: Policy, Policies

Give feedback

Help improve this page

All services > Policy

Policy | Definitions

...

The screenshot shows the 'Policy | Definitions' blade in the Azure portal. The left sidebar has sections for Overview, Compliance, Remediation, Events, and Authoring, with 'Definitions' selected. Under 'Definitions', there are sub-sections for Assignments, Machine Configuration, and Exemptions. The main area displays a table of policy definitions. The columns are: Name, Latest version, Definition location, Policy type, Type, Definition type, and Category. The table lists various built-in policies like 'Microsoft Managed Control 1599 - Developer Configuration', 'Audit virtual machines without disaster recovery config', etc. A note at the top of the table says: 'The maximum number of definitions that can be displayed are shown, and some definitions might not be visible. Please use filters to narrow down your selection.' At the bottom of the table, it says '[Preview]: Configure VMSS created with Shared Image G 2.1.0-preview'.

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 size 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, keep the default Scope. Setting Scope Value Use default selected Policy definition click elipses then search Allowed Locations then Select Assignment Name Allowed Locations

Specific subsets of resources can expand to learn more.

Basics

Policy definition * ...

Version (preview) * ...

Overrides [\(Expand\)](#) Using overrides, you can change the effects or referenced versions of definitions for all or a subset of resources evaluated by this assignment. Expand to learn more.

Assignment name *

Description

Policy enforcement Enabled

6. On the Parameters tab, select Japan West. Click Review + create, and then Create. 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.

Assign policy

X

Basics

Parameters

Remediation

Non-compliance messages

Review + create

 Search by parameter name

Only show parameters that need input or review

Allowed locations *

Japan West

▼

Previous

Next

Review + create

 Give feedback

Exclusions are optional. 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.

7. 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).

 Creating policy assignment succeeded

X

Creating policy assignment 'Allowed locations' in 'Azure subscription 1' was successful. Please note that the assignment takes around 5-15 minutes to take effect.

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 + 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 Subscription Resource group Value Use the default supplied myRGPolicy (create new) Storage account name storageaccountxxxx 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.

The screenshot shows the 'Create a storage account' page in the Azure portal. At the top, there's a red validation error message: 'Validation failed. Required information is missing or not valid.' Below the message, the 'Review + create' tab is selected. The 'Basics' section contains the following configuration:

Subscription	Azure subscription 1
Resource group	myRGPolicy
Location	East US
Storage account name	storageaccount2280
Preferred storage type	
Performance	Standard
Replication	Read-access geo-redundant storage (RA-GRS)

The 'Advanced' section contains the following settings:

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

At the bottom, there are 'Previous', 'Next', and 'Create' buttons.

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 Allowed Locations It will open an Allowed locations Policy Compliance window.

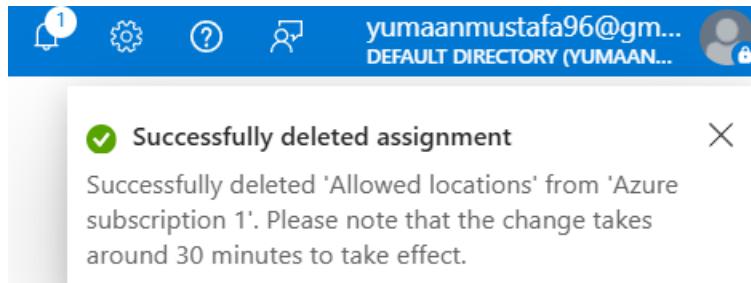
The screenshot shows the 'Allowed locations' policy assignment details. The 'Essentials' section includes:

Name	: Allowed locations	Scope	: Azure subscription 1
Definition version (preview)	: 1.*.*	Excluded scopes	: --
Description	: --	Definition type	: Policy
Assignment ID	: /subscriptions/a3e17407-645b-4443-990f-e8d6df69025c/providers/microsoft.auth...	Policy enforcement	: Default
Assigned by	: --		

The 'Parameters' section shows a single parameter:

Parameter ID	Parameter name	Parameter value	Policy assignment parameter reference
listOfAllowedLocations	Allowed locations	["japanwest"]	User defined parameter

3. Click Delete Assignment in the top menu. Confirm you wish to delete the policy assignment by clicking Yes



4. Try to create another storage account to ensure the policy is no longer in effect.

Location	East US
Storage account name	storageaccount2280133
Preferred storage type	
Performance	Standard
Replication	Locally-redundant storage (LRS)

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

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

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 optionally remove this resource group. Search for resource groups, click your resource group, and then click Delete resource group. Verify the name of the resource group and then click Delete. Monitor the Notifications to see how the delete is proceeding.