



Azure Policy

Azure Policy is a service in Microsoft Azure that helps you manage and enforce organizational policies across your Azure resources. It allows you to create, assign, and manage policies that ensure your resources comply with organizational standards and service level agreements (SLAs). Here are some key aspects of Azure Policy:

1. **Policy Definition:** You can define policies using JSON format. These definitions specify the conditions under which the policy is enforced and the actions that are taken when the policy conditions are met.
2. **Policy Assignment:** Policies are assigned to specific scopes, which can be a subscription, resource group, or individual resources. Once assigned, the policy evaluates resources within that scope to ensure compliance.
3. **Policy Compliance:** Azure Policy continuously evaluates resources for compliance. It provides detailed compliance reports and dashboards to help you understand the compliance state of your resources.
4. **Built-in Policies:** Azure provides a wide range of built-in policy definitions for common scenarios, such as restricting certain types of resources, enforcing tagging conventions, and ensuring resource configurations meet security standards.
5. **Custom Policies:** In addition to built-in policies, you can create custom policies to address specific needs within your organization.
6. **Policy Initiatives:** A policy initiative is a collection of policies that are grouped together to achieve a specific goal. By using initiatives, you can simplify the assignment and management of multiple policies.
7. **Policy Enforcement Modes:** Policies can be enforced in different modes:
 - **Audit:** Logs non-compliant resources without preventing their creation or modification.
 - **Deny:** Prevents the creation or modification of resources that do not comply with the policy.
 - **Append:** Adds additional properties to resources during creation or update to ensure compliance.
 - **DeployIfNotExists:** Deploys a specified resource if it does not already exist to bring non-compliant resources into compliance.

Azure Policy is an essential tool for ensuring that your Azure environment remains compliant with organizational and regulatory requirements, helps in maintaining governance, and enables automation of compliance management.



Use Cases of Azure Policy

Azure Policy is a versatile tool used to enforce various organizational and compliance requirements across Azure resources. Here are some common use cases:

1. Governance and Compliance:

- **Enforcing Resource Tagging:** Ensure all resources are tagged with required metadata, such as cost center, environment, or owner.
- **Compliance with Regulatory Standards:** Enforce configurations that align with standards like GDPR, HIPAA, and ISO 27001 by ensuring that necessary security controls are in place.

2. Security:

- **Restricting Public Endpoints:** Prevent resources from being publicly accessible by ensuring virtual machines, storage accounts, or databases do not have public IP addresses.
- **Enforcing Network Security Rules:** Ensure that network security groups (NSGs) have specific inbound and outbound rules for secure communication.

3. Cost Management:

- **Resource Type Restrictions:** Prevent the creation of costly resource types, such as large VM sizes, to control spending.
- **Location Restrictions:** Restrict resource deployment to specific regions to optimize costs or comply with data residency requirements.

4. Operational Best Practices:

- **Ensuring Backup and Recovery:** Ensure that critical resources, like VMs and databases, have backup policies configured.
- **Monitoring and Logging:** Enforce the enablement of monitoring and logging services, such as Azure Monitor and Azure Security Center, across all resources.

5. Resource Configuration:

- **Enforcing Naming Conventions:** Ensure resources follow a specific naming convention for better organization and management.
- **Resource SKU Enforcement:** Restrict the use of certain SKUs for resources like VMs and storage accounts to enforce standards and control costs.

6. DevOps and Automation:

- **Infrastructure as Code (IaC) Compliance:** Ensure that infrastructure deployed through IaC templates (e.g., ARM templates, Terraform) complies with organizational policies.
- **Deployment Guardrails:** Implement guardrails in CI/CD pipelines to ensure that only compliant resources are deployed.

7. Resource Cleanup:

- **Orphaned Resources Identification:** Identify and report resources that are not associated with any workload or application, helping to clean up unused resources.
8. **Hybrid and Multi-Cloud Management:**
- **Consistent Policies Across Environments:** Apply the same policies across on-premises and multi-cloud environments using Azure Arc to ensure consistent governance.

What are we doing in this Lab?

In this lab, you are learning how to use Azure Policy to enforce organizational standards and ensure compliance across your Azure resources. The goal is to familiarize you with creating, assigning, and managing policies within the Azure environment. Here's a summary of the steps and the end goal:

Summary:

1. **Explore Azure Policy:** Navigate to the Azure Policy service in the Azure Portal.
2. **Understand Built-in and Custom Policies:** Learn the difference between policies and initiatives, and review built-in policy definitions.
3. **Assign a Policy:** Assign a policy (e.g., "Allowed Locations") to restrict resource creation to a specific region.
4. **Verify Compliance:** Confirm that the policy prevents the creation of resources outside the allowed region.
5. **Create and Assign Another Policy:** Assign a policy to automatically add or replace tags on resources.
6. **Test Policy Enforcement:** Create resources to see if the policies are correctly enforced (e.g., location restriction and automatic tagging).

End Goal:

The end goal is to ensure you understand how to use Azure Policy to maintain governance, enforce compliance, and automate policy management across your Azure resources. By completing these steps, you'll be able to manage and enforce organizational standards effectively, ensuring your Azure environment remains compliant with your corporate policies and regulatory requirements.

To begin with the Lab:

1. Azure Policy is a service in Azure that you use to create, assign, and manage policy definitions.
2. Policy definitions enforce different rules and actions over your resources, so those resources stay compliant with your corporate standards and service level agreements.
3. Azure does this by running an evaluation of your resources and scanning for those not compliant with the policy definitions you have. For example, you can have a policy to

allow only certain types of virtual machines. Another requires that all resources have a particular tag. These policies are then evaluated when creating and updating resources.

4. Now in your Azure Portal you search for Azure Policy and navigate to it.
5. So, if you are visiting on Policy service for the first time then its dashboard will look like this.
6. Now if you go to definitions as it is highlighted in the snapshot.

The screenshot shows the Azure Policy dashboard. At the top, there's a search bar and a scope filter set to 'Free Trial'. On the left, a sidebar lists 'Overview', 'Getting started', 'Compliance', 'Remediation', 'Events', 'Authoring' (with 'Definitions' highlighted by a red box), 'Assignments', and 'Exemptions'. The main area displays 'Overall resource compliance' at 100%, 'Resources by compliance state' (0 compliant, 0 non-compliant), 'Non-compliant initiatives' (0 out of 0), and 'Non-compliant policies' (0 out of 0). A 'Learn more' link is present. Below this, a table lists 'ASSIGNMENTS BY COMPLIANCE (LAST 7 DAYS)' with columns for Name, Scope, Compliance state, Resource compliance, Non-compliant resources, and Non-compliant policies. A 'View all' link is at the bottom.

7. So, first here you will see the Built-in Initiatives, and if you scroll down then you will be able to see the Built-in Policies.
8. Also, the basic difference between policies and initiatives is that the initiatives are the collection of policy, so instead of applying a single policy you can apply a initiative which have multiple policies in it.

The screenshot shows the 'Policy | Definitions' page. The left sidebar is identical to the dashboard. The main area has a search bar and filters for 'Scope: Free Trial', 'Definition type: All definition types', 'Policy type: All policy types', and 'Category: All categories'. It includes a note about the maximum number of definitions. A table lists 'Name', 'Latest versi...', 'Definition location', 'Poli...', 'Type', 'Definition t...', and 'Category'. The table contains numerous entries such as 'Enable Azure Monitor for VMSS with Azure Monitoring', 'Audit Public Network Access', and various FedRAMP and security-related items. A '...' button is at the bottom right of the table.

9. Now in the search option search for allowed locations, so you will see a policy which is also highlighted in the snapshot. Click on it.

10. Then you will be inside a policy, here you can see its definition written in JSON format, and then you will see that it has been assigned to nothing as it has zero assignment. Now click on Assign Policy.

```

1  "properties": {
2   "displayName": "Allowed locations",
3   "policyType": "BuiltIn",
4   "mode": "Indexed",
5   "description": "This policy enables you to restrict the locations your organization can specify when deploying resources. Use to enforce your geo-compliance requirements.",
6   "metadata": {
7     "version": "1.0.0",
8     "category": "General"
9   },
10  "version": "1.0.0",
11  "parameters": {
12    "listOfAllowedLocations": {
13      "type": "Array",
14      "metadata": {
15        "description": "The list of locations that can be specified when deploying resources."
16      }
17    }
18  }
19}

```

11. Now you need to choose your scope, so just choose your subscription then leave everything as it is and move to next page.

Assign policy

Basics Parameters Remediation Non-compliance messages Review + create

Scope

Scope * ...

[Learn more about setting the scope](#)

Exclusions

Optionally select resources to exclude from the policy assignment. ...

Resource selectors [\(Expand\)](#) Using resource selectors, you can further refine this assignment's applicability by targeting specific subsets of resources. 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 * ①

Description

12. Then in the parameters we need to allow a location of our choice. Let's say we are allowing a location from India and it is only Central India is allowed rest are not allowed.
13. After that just move to review page and create your Policy.

Home > Policy | Definitions > Allowed locations >

Assign policy

Basics **Parameters** Remediation Non-compliance messages Review + create

Search by parameter name Only show parameters that need input or review

Allowed locations * ▼

X
 All
 Central India
 Jio India West
 Jio India Central
 South India
 West India

14. Once you have assigned the policy then you will see that in the assignment it is showing you to which scope it has been assigned.

Allowed locations ...

Policy definition

[Assign policy](#) [Edit definition](#) [Duplicate definition](#) [Select version \(preview\)](#) [Delete definition](#)

[Essentials](#)

Name	: Allowed locations	Definition location	: --
Version (preview)	: 1.0.0	Definition ID	: /providers/Microsoft.Authorization/policyDefinitions/e56962a6-4747-49cd-b67b...
Description	: This policy enables you to restrict the locations your organization can specify when creating resources.		
Available Effects	: Deny	Type	: Built-in
Category	: General	Mode	: Indexed

Definition [Assignments \(1\)](#) [Parameters \(1\)](#)

(1) You are viewing assignment(s) for all versions of this policy definition.

Assignment name	Scope	Assigned by	Version (preview)	...
Allowed locations	Free Trial	1.0.0	...	

15. Then if you go to the overview of Policy, you will see that our policy is in compliant state.

Home > **Policy** ...

Search Scope: Free Trial

[Overview](#)

Getting started Compliance Remediation Events

Authoring

- Definitions
- Assignments
- Exemptions

Overall resource compliance: **100%**

Resources by compliance state: 0 - Compliant (0) 0 - Non-compliant (0)

Non-compliant initiatives: 0 out of 0

Non-compliant policies: 0 out of 1

LEARN MORE

[Learn about Policy](#) [Onboarding tutorial](#)

Name	Scope	Compliance state	Resource compli...	Non-compliant resources	Non-compliant policies
Allowed locations	Free Trial	Compliant	100% (0 out of 0)	0	0

[View all](#)

16. Now to confirm whether it is working or not. Let's go to the resource group and create one.

Create a resource group

Basics Tags Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)

Project details

Subscription * [\(i\)](#)

Free Trial



Resource group * [\(i\)](#)

demo-RG



Resource details

Region * [\(i\)](#)

(Asia Pacific) Central India



17. Once the resource group is created then we are going to create a resource in it let's say a storage account. Here we are going to choose West India as its location.

Create a storage account

Iables. 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 *	Free Trial
Resource group *	demo-RG
	Create new

Instance details

Storage account name * ⓘ	demostorage221133
Region * ⓘ	(Asia Pacific) West India
Performance * ⓘ	<input checked="" type="radio"/> Standard: Recommended for most scenarios (general-purpose v2 account) <input type="radio"/> Premium: Recommended for scenarios that require low latency.
Redundancy * ⓘ	Locally-redundant storage (LRS)

[Previous](#)

[Next](#)

Review + create

18. Below you can see that the validation has been failed.

Create a storage account

 [Validation failed. View error details →](#)

[Basics](#) [Advanced](#) [Networking](#) [Data protection](#) [Encryption](#) [Tags](#) [**Review + create**](#)

[View automation template](#)

Basics

Subscription	Free Trial
Resource group	demo-RG
Location	West India
Storage account name	demostorage221133
Performance	Standard
Replication	Locally-redundant storage (LRS)

19. And if you try to see the error then you can see that it has failed because of our Allowed locations Policy.

Errors



[Summary](#) [Raw Error](#)

ERROR DETAILS



Resource 'demostorage221133' was disallowed by policy. (Code: RequestDisallowedByPolicy)

Policy: [Allowed locations](#)

WAS THIS HELPFUL?

Troubleshooting Options

[New Support Request](#)

20. Now we'll try another example, again go to definitions and search for the policy mention below for add or replace a tag on resources.

Home > Policy

Policy | Definitions ...

x << + Policy definition + Initiative definition Refresh

Overview Getting started Compliance Remediation Events Authoring

Definitions Assignments Exemptions

Search Scope : Free Trial Definition type : All definition types Policy type : All policy types Category : All categories

Name	Latest versi...	Definition location	Poli...	Type	Definition t...	Category
Add or replace a tag on resources	1.0.0		Builtin	Policy	Tags	

21. Again, you can see the definition of this policy, now click on assign policy.

The screenshot shows the 'Add or replace a tag on resources' policy definition in the Azure portal. It includes the policy's name, version, description, available effects, category, and its JSON definition. The JSON code defines a policy named 'Add or replace a tag on resources' with a display name, policy type (Builtin), mode (Indexed), and a detailed description. It specifies parameters for tag name, type (String), and metadata, including a display name.

22. No change for the basic settings just leave everything as it is and move to next option.

Assign policy ...

The screenshot shows the 'Assign policy' wizard in the 'Basics' step. It includes tabs for Basics, Parameters, Remediation, Non-compliance messages, and Review + create. Under the Basics tab, there are sections for Scope, Exclusions, Resource selectors, and Overrides. The Scope section shows 'Free Trial' assigned. The Exclusions section is empty. The Resource selectors section indicates that resource selectors can refine the assignment's applicability. The Overrides section indicates that overrides can change the effects or referenced versions of definitions. The Assignment name field is set to 'Add or replace a tag on resources'. The Description field is empty. At the bottom, there are 'Previous' and 'Next' buttons, and a prominent 'Review + create' button.

23. Then here you need to define the tag name and value of your choice as you can see below.

Assign policy ...

Basics **Parameters** Remediation Non-compliance messages Review + create

Search by parameter name Only show parameters that need input or review

Tag Name * ⓘ

Department

Tag Value * ⓘ

Information Technology

24. Now in the remediation you need to allow it then move to the review page and create your policy.

Assign policy ...

Basics Parameters **Remediation** Non-compliance messages Review + create

By default, this assignment will only take effect on newly created resources. Existing resources can be updated via a remediation task after the policy is assigned. For deployIfNotExists policies, the remediation task will deploy the specified template. For modify policies, the remediation task will edit tags on the existing resources.

Create a remediation task

Policy to remediate

Add or replace a tag on resources

Managed Identity

Policies with the deployIfNotExists and modify effect types need the ability to deploy resources and edit tags on existing resources respectively. To do this, choose between an existing user assigned managed identity or creating a system assigned managed identity. [Learn more about Managed Identity](#).

Create a Managed Identity ⓘ



Type of Managed Identity ⓘ

System assigned managed identity

User assigned managed identity

System assigned identity location

(Asia Pacific) Central India

25. Now we will create a resource which is a storage account. But this time we will create it in Central India as it is the only location allowed.

26. So, go to storage account and click on create. Now give it a name choose your location and move to review page then create your storage account.

Project details

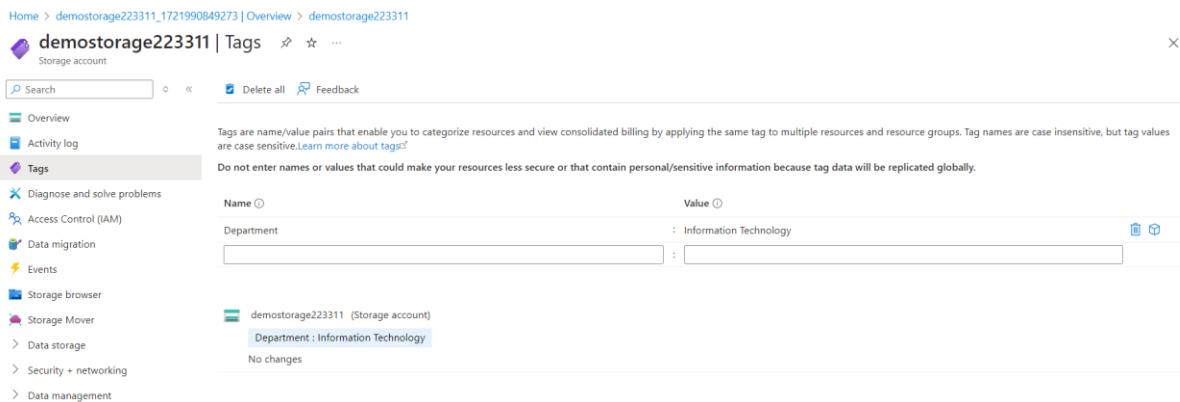
Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription *	Free Trial
Resource group *	demo-RG
	Create new

Instance details

Storage account name * ⓘ	demostorage223311
Region * ⓘ	(Asia Pacific) Central India
	Deploy to an Azure Extended Zone
Performance * ⓘ	<input checked="" type="radio"/> Standard: Recommended for most scenarios (general-purpose v2 account) <input type="radio"/> Premium: Recommended for scenarios that require low latency.
Redundancy * ⓘ	Locally-redundant storage (LRS)

27. Once your storage account is created then go to it and navigate to tags. Below you can see that the tag has been automatically attached to our storage account.



The screenshot shows the 'Tags' section of the Azure Storage Account overview page for 'demostorage223311'. The left sidebar includes links for Overview, Activity log, Tags (which is selected), Diagnose and solve problems, Access Control (IAM), Data migration, Events, Storage browser, Storage Mover, Data storage, Security + networking, and Data management. The main content area displays a table for adding tags. A note states: 'Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Tag names are case insensitive, but tag values are case sensitive.' It also cautions against entering sensitive information. A single tag is listed: 'Department : Information Technology'. At the bottom, it says 'No changes'.