



Ensure Azure Resource Compliance with Azure Policy

A hands-on governance lab demonstrating how to enforce compliant resource deployment using Azure Policy.

What you'll learn:

- Why Azure Policy matters in Governance
- How to assign a policy at resource-group scope
- How compliance is evaluated
- How Azure prevents non-compliant deployments
- Real-world Architect use cases



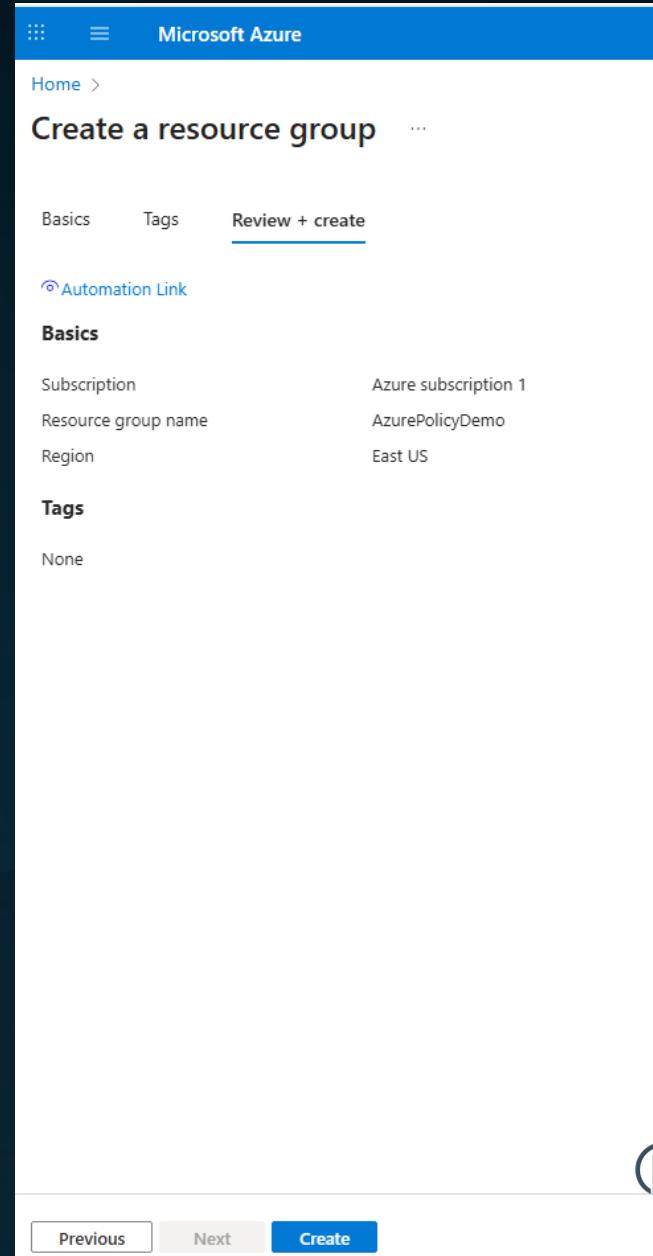
Why Azure Policy Matters (Architect View)

Azure Policy allows architects to **enforce organizational standards** and **prevent drift** across all cloud resources.

Azure Policy solves these problems:

- Prevent resources from being created in unauthorized regions
- Ensure security baselines (encryption, tags, SKUs, networking)
- Maintain regulatory compliance (ISO, NIST, CIS)
- Provide continuous compliance visibility across subscriptions

This lab demonstrates a classic enterprise control:
→ Restrict resources to deploy only in East US



Home > Create a resource group

Basics Tags Review + create

Automation Link

Basics

Subscription	Azure subscription 1
Resource group name	AzurePolicyDemo
Region	East US

Tags

None

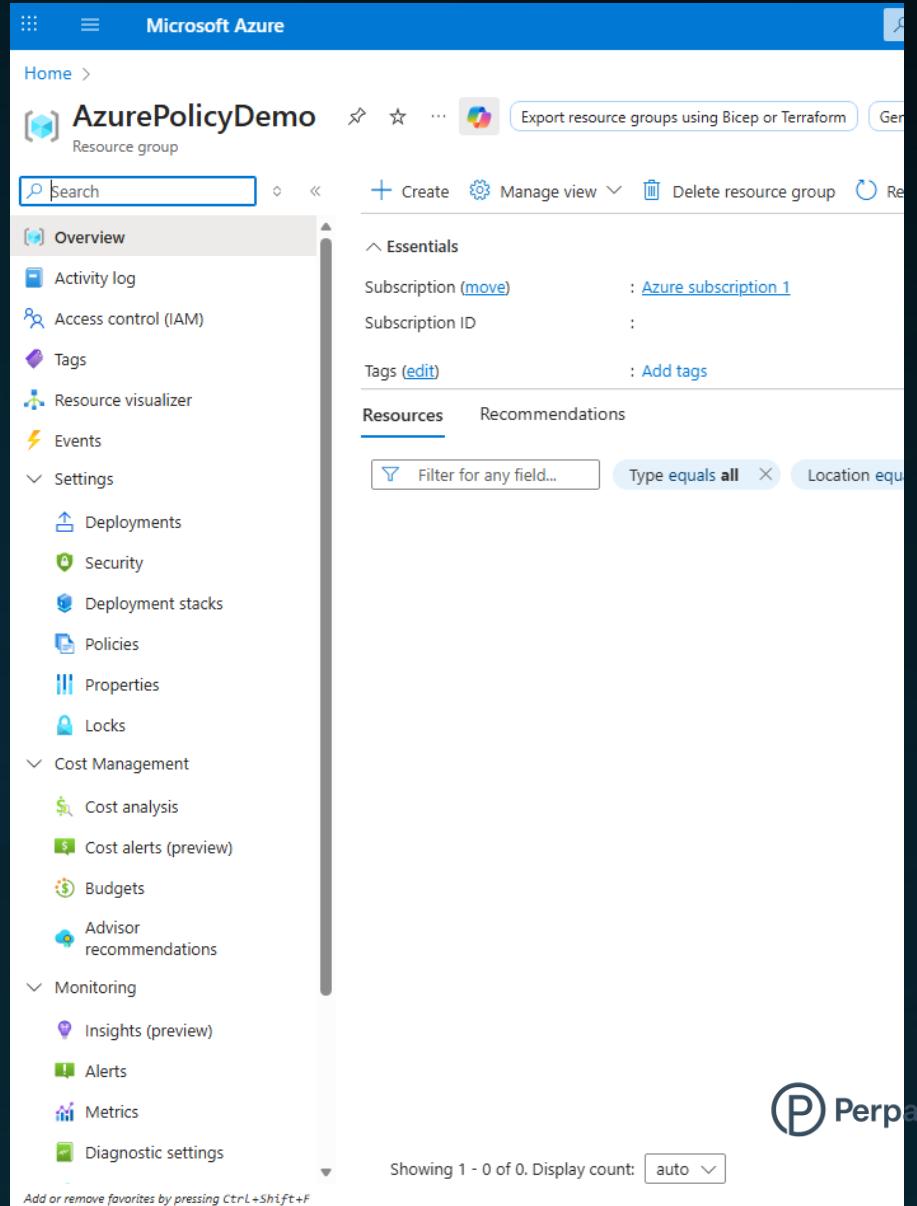
Create a Dedicated Resource Group

We start by creating an isolated resource group for the policy demo.

Steps:

1. Portal → *Resource groups* → *Create*
2. Name: **AzurePolicyDemo**
3. Region: **East US**
4. Review + create

This RG acts as a test environment where the policy will be applied.



Microsoft Azure

Home > AzurePolicyDemo Resource group

Search

Overview

Activity log

Access control (IAM)

Tags

Resource visualizer

Events

Settings

- Deployments
- Security
- Deployment stacks
- Policies
- Properties
- Locks

Cost Management

- Cost analysis
- Cost alerts (preview)
- Budgets
- Advisor recommendations

Monitoring

- Insights (preview)
- Alerts
- Metrics
- Diagnostic settings

Subscription (move) : Azure subscription 1

Subscription ID :

Tags (edit) : Add tags

Resources Recommendations

Filter for any field... Type equals all

Showing 1 - 0 of 0. Display count: auto

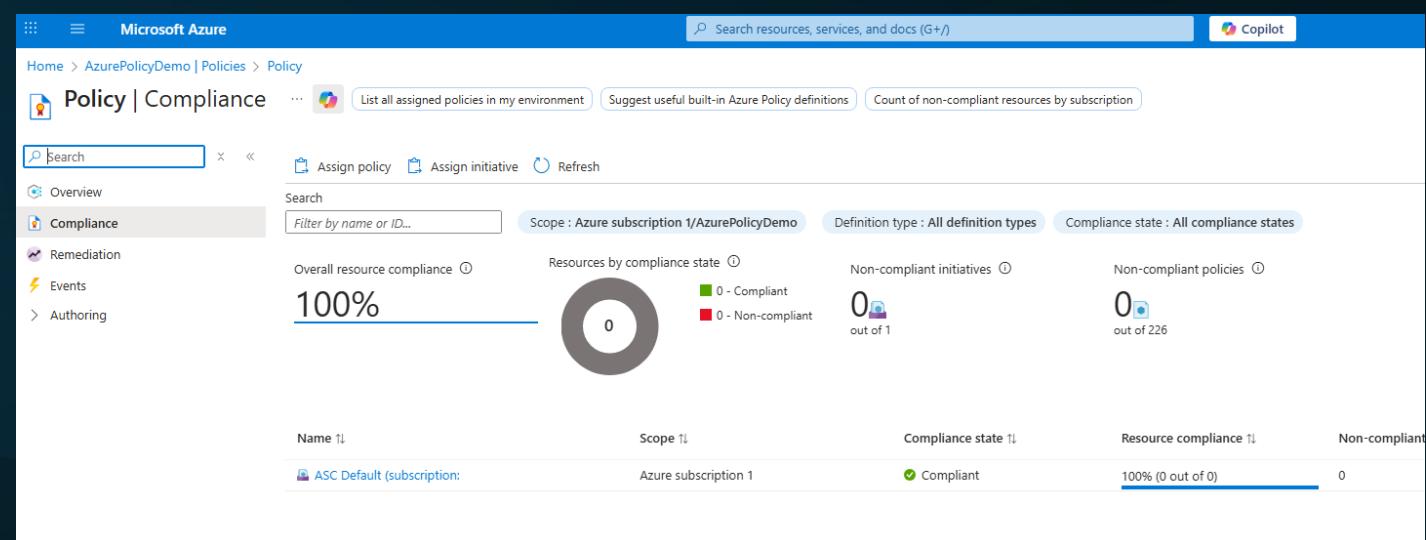
Azure Policy Compliance Dashboard

Azure Policy gives a compliance score and shows current evaluations.

Before assigning any policy, compliance will be 100% because no resources exist.

Architect Insight:

Compliance is **not instant**—Azure may take minutes to reflect the evaluation.



Assign a New Policy

Navigate to:
Resource Group → **Policies** → *Assign policy*.

Here we define:

- **Scope** (AzurePolicyDemo RG)
- **Policy Definition** (what rule will apply)
- **Assignment Name** (label for the policy)
- Optional remediation tasks

This is where governance becomes automated.

The screenshot shows the 'Assign policy' interface in the Microsoft Azure portal. The 'Basics' tab is selected. The 'Scope' section is set to 'Azure subscription 1/AzurePolicyDemo'. The 'Policy definition' field is empty. The 'Assignment name' field is also empty. The 'Description' field is empty. The 'Policy enforcement' toggle is set to 'Enabled'. On the right, a sidebar titled 'Available Definitions' lists various Azure policies, including 'Microsoft Managed Control 1599 - Developer Configuration', 'Audit virtual machines without disaster recovery', and 'Microsoft Managed Control 1375 - Incident Response'. The bottom right corner features the PerparimLabs logo.

© PerparimLabs | Azure Governance | Microsoft Cloud Architect

Select the Policy Definition

Search for the keyword: **location**

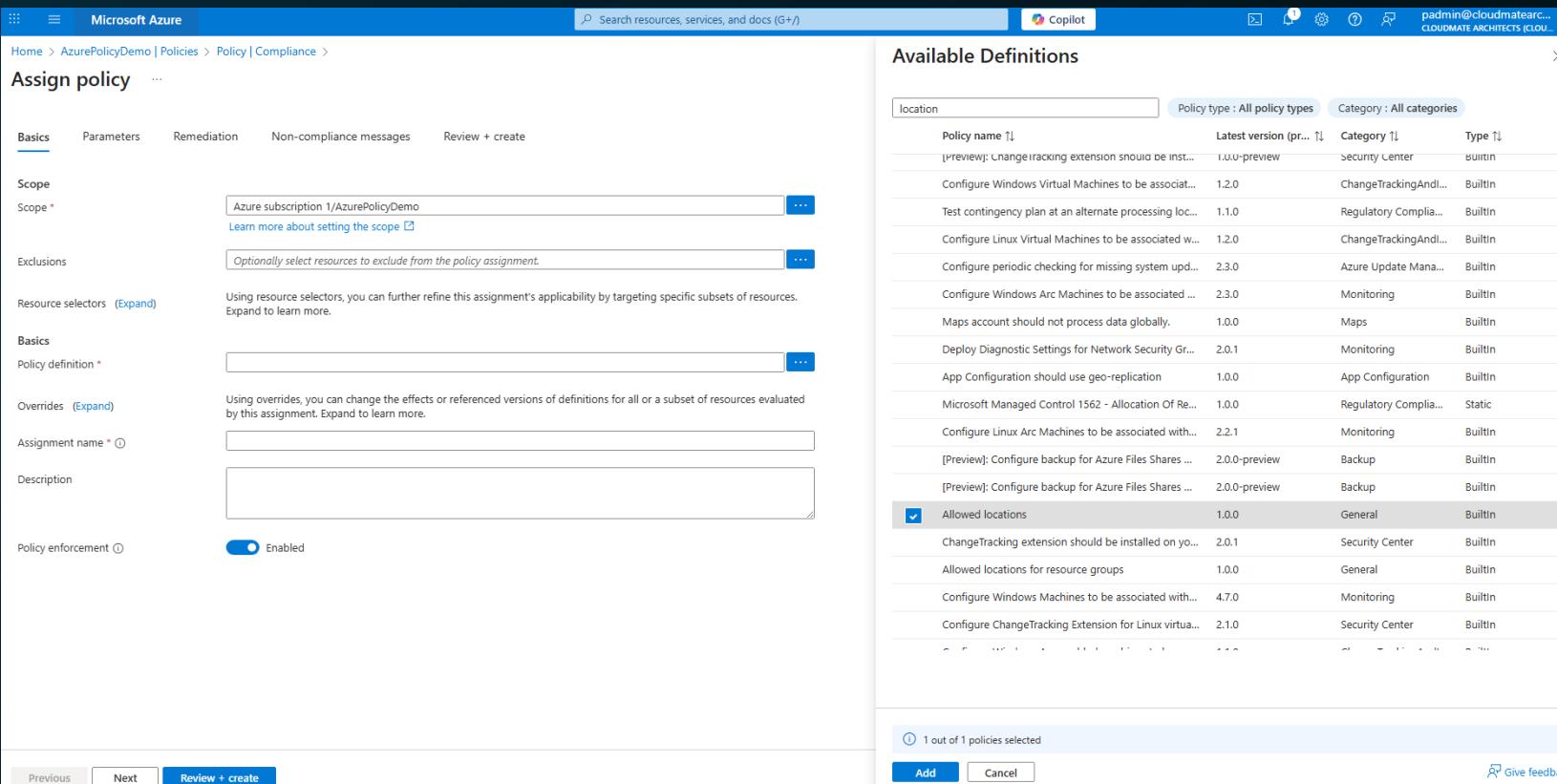
Choose:

✓ Allowed Locations (built-in)

This policy enforces that all deployed resources must be created in approved regions.

Architect Insight:

This is one of the most widely used enterprise governance policies.



The screenshot shows the 'Assign policy' screen in the Microsoft Azure portal. The 'Basics' tab is selected. The 'Scope' section shows 'Azure subscription 1/AzurePolicyDemo' as the assigned scope. The 'Available Definitions' pane on the right is filtered for 'location' and shows a list of built-in policies. The 'Allowed locations' policy is selected, indicated by a checked checkbox. The list includes various built-in policies from categories like Security Center, Change Tracking, and Monitoring.

Policy name	Latest version	Category	Type
[Preview]: Change tracking extension should be installed on yo...	1.0.0-preview	Security Center	Builtin
Configure Windows Virtual Machines to be associated with...	1.2.0	ChangeTrackingAnd...	Builtin
Test contingency plan at an alternate processing loc...	1.1.0	Regulatory Complia...	Builtin
Configure Linux Virtual Machines to be associated with...	1.2.0	ChangeTrackingAnd...	Builtin
Configure periodic checking for missing system upd...	2.3.0	Azure Update Mana...	Builtin
Configure Windows Arc Machines to be associated with...	2.3.0	Monitoring	Builtin
Maps account should not process data globally.	1.0.0	Maps	Builtin
Deploy Diagnostic Settings for Network Security Gr...	2.0.1	Monitoring	Builtin
App Configuration should use geo-replication	1.0.0	App Configuration	Builtin
Microsoft Managed Control 1562 - Allocation Of Re...	1.0.0	Regulatory Complia...	Static
Configure Linux Arc Machines to be associated with...	2.2.1	Monitoring	Builtin
[Preview]: Configure backup for Azure Files Shares ...	2.0.0-preview	Backup	Builtin
[Preview]: Configure backup for Azure Files Shares ...	2.0.0-preview	Backup	Builtin
<input checked="" type="checkbox"/> Allowed locations	1.0.0	General	Builtin
ChangeTracking extension should be installed on yo...	2.0.1	Security Center	Builtin
Allowed locations for resource groups	1.0.0	General	Builtin
Configure Windows Machines to be associated with...	4.7.0	Monitoring	Builtin
Configure ChangeTracking Extension for Linux virtua...	2.1.0	Security Center	Builtin

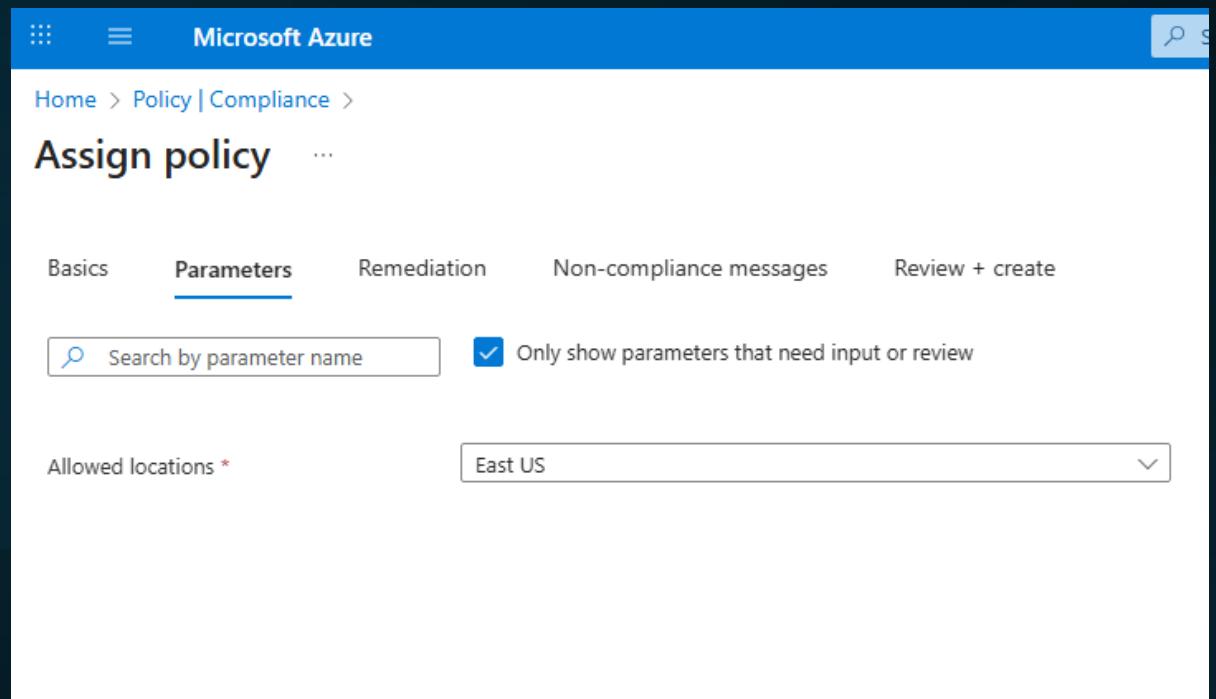
Configure the Policy Parameters

The Allowed Locations policy requires specifying the permitted region(s).

For this lab:

→ **Allowed locations: East US**

Once assigned, Azure will deny deployments outside East US.



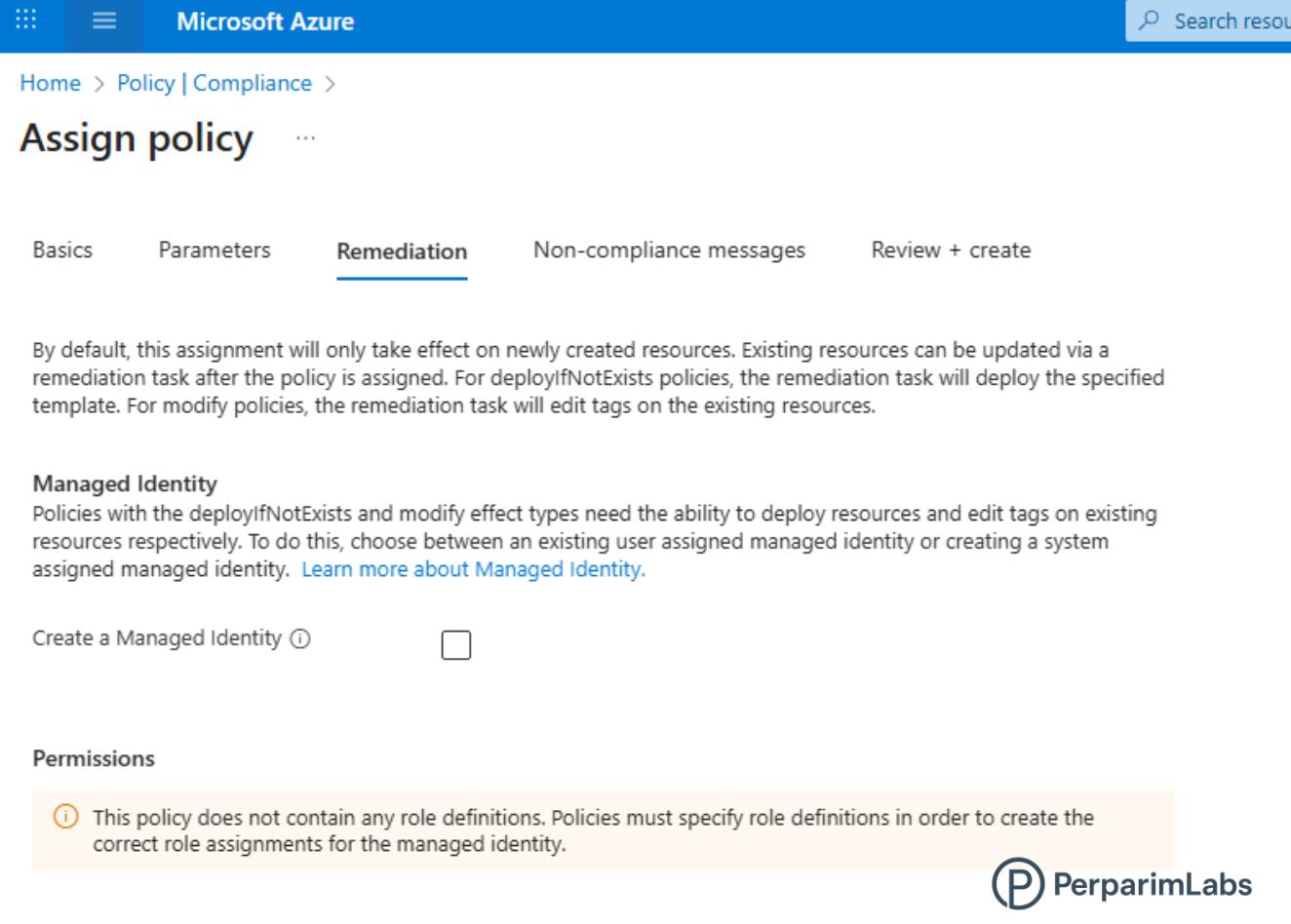
Remediation Settings

Remediation tasks do not apply here because:

- Deny policies block at creation
- Existing resources cannot be “moved” by policy
- Azure will simply mark existing non-compliant resources

This aligns with best practice governance:

Prevent drift early instead of fixing it later.



The screenshot shows the Microsoft Azure Policy | Compliance interface. The page title is "Assign policy". Below the title, there are tabs: Basics, Parameters, **Remediation**, Non-compliance messages, and Review + create. The Remediation tab is selected. A description states: "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." Under the "Managed Identity" section, it says: "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." A link "Learn more about Managed Identity" is provided. Below this, there is a checkbox labeled "Create a Managed Identity" with an information icon. The "Permissions" section contains a note: "This policy does not contain any role definitions. Policies must specify role definitions in order to create the correct role assignments for the managed identity." The note has an information icon and is highlighted with a yellow background.

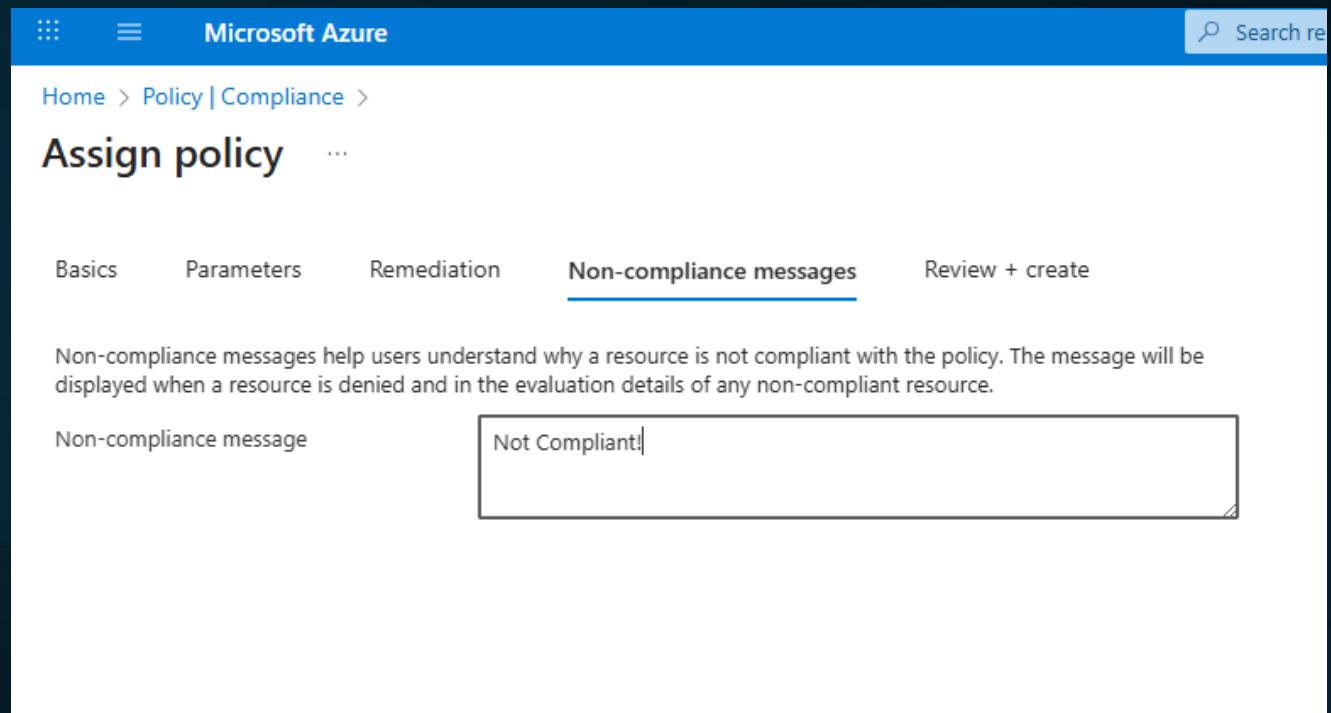
Non-Compliance Message

Add a helpful message for users attempting non-compliant deployments.

Example:

“Not Compliant – Resource region must be East US.”

This improves DevOps feedback loops.



Review & Create

Policy Assignment Summary:

- **Scope:** AzurePolicyDemo
- **Policy:** Allowed locations
- **Parameter:** East US
- **Effect:** Deny
- **Non-compliance message:** Not Compliant

Click **Create** to activate governance.

Microsoft Azure

Home > Policy | Compliance > Assign policy

Basics Parameters Remediation Non-compliance messages Review + create

Basics

Scope	Azure subscription 1/AzurePolicyDemo
Exclusions	--
Policy definition	Allowed locations
Assignment name	Allowed locations
Version (preview)	1.0.0
Description	--
Policy enforcement	Default
Assigned by	Perparim Abdullahu

Advanced

Resource selectors	No selectors associated with this assignment.
Overrides	No overrides associated with this assignment.

Parameters

Allowed locations	["eastus"]
-------------------	------------

Remediation

Create a Managed Identity	No managed identity associated with this assignment.
---------------------------	--

Non-compliance messages

Default non-compliance message	Not Compliant!
--------------------------------	----------------

Review + create

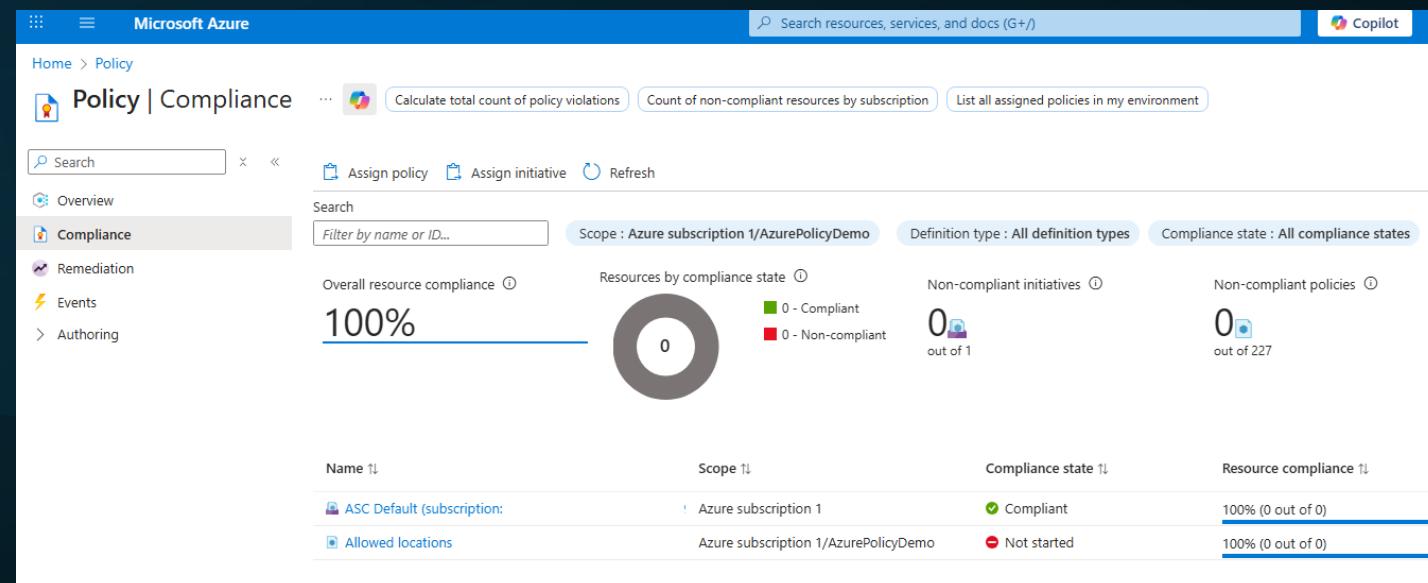
Cancel Microsoft Create



Compliance Evaluation

Azure Policy now evaluates your resource group.
Because no resources exist, everything appears
100% compliant.

Architect Insight:
Policy evaluation is continuous and updates as
resources change.



Test the Policy with a Storage Account (Fail Case)

Attempt to create a storage account *outside* the allowed region.

Example:

Region: **West US 2**

Policy applies → Azure immediately blocks the deployment

Error: **Not Compliant!**

This proves the policy is actively enforcing governance.

The screenshot shows the 'Create a storage account' wizard in the Microsoft Azure portal. The 'Basics' tab is selected. In the 'Project details' section, the 'Subscription' is set to 'Azure subscription 1' and the 'Resource group' is set to 'AzurePolicyDemo' (with a 'Create new' option). In the 'Instance details' section, the 'Storage account name' field is empty. The 'Region' dropdown is set to '(US) West US 2', which is highlighted in red with a tooltip 'Not Compliant! (Policy details)'. Below the region dropdown, there is a note: 'This helps us provide relevant guidance. It doesn't restrict your storage to this resource type. Learn more'. Under 'Preferred storage type', the 'Standard' radio button is selected. In the 'Performance' section, the 'Standard' radio button is also selected. In the 'Redundancy' section, 'Geo-redundant storage (GRS)' is selected, and a checkbox for 'Make read access to data available in the event of regional unavailability' is checked. At the bottom, there are 'Previous', 'Next', and 'Review + create' buttons, with 'Review + create' being the active button.

Test the Policy Again (Success Case)

Deploy the same storage account but this time select:

→ **Region: East US**

The deployment succeeds because it aligns with the policy.

This confirms your Azure governance control is working correctly.

Microsoft Azure

Home > Create a storage account

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. 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 * Azure subscription 1

Resource group * AzurePolicyDemo

Storage account name * (empty)

Region * (US) East US

Deploy to an Azure Extended Zone

Preferred storage type Choose preferred storage type

This helps us provide relevant guidance. It doesn't restrict your storage to this resource type. [Learn more](#)

Performance * Standard: Recommended for most scenarios (general-purpose v2 account)

Premium: Recommended for scenarios that require low latency.

Redundancy * Geo-redundant storage (GRS)

Make read access to data available in the event of regional unavailability.

Geo priority replication guarantees Blob storage data is geo-replicated within 15 minutes.

Previous Next Review + create

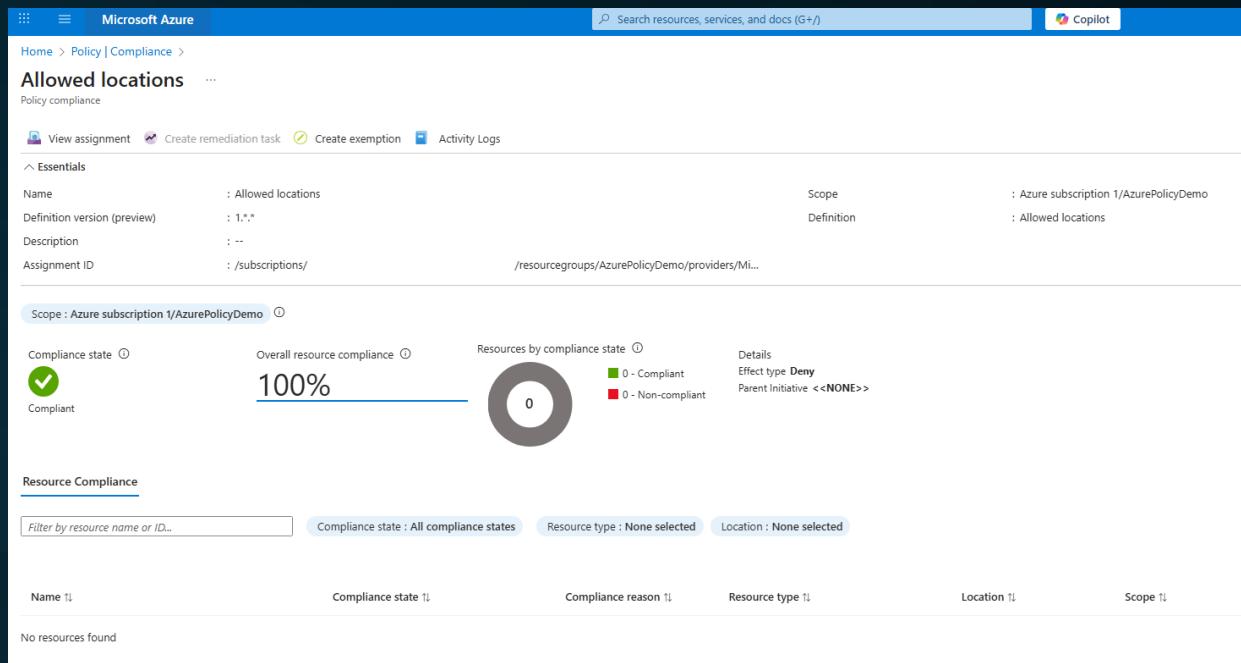
Policy Compliance Dashboard (After Enforcement)

Return to the Allowed Locations policy.

You see:

- **Compliance: 100%**
- The resource group is compliant
- Azure prevented drift before it happened

This is how enterprise cloud teams maintain control at scale.



Clean Up the Lab

Delete the resource group to reset your environment.

This will remove:

- Storage account
- Policy assignment
- All related resources

Always clean up to avoid unnecessary costs.

