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

PerparimLabs

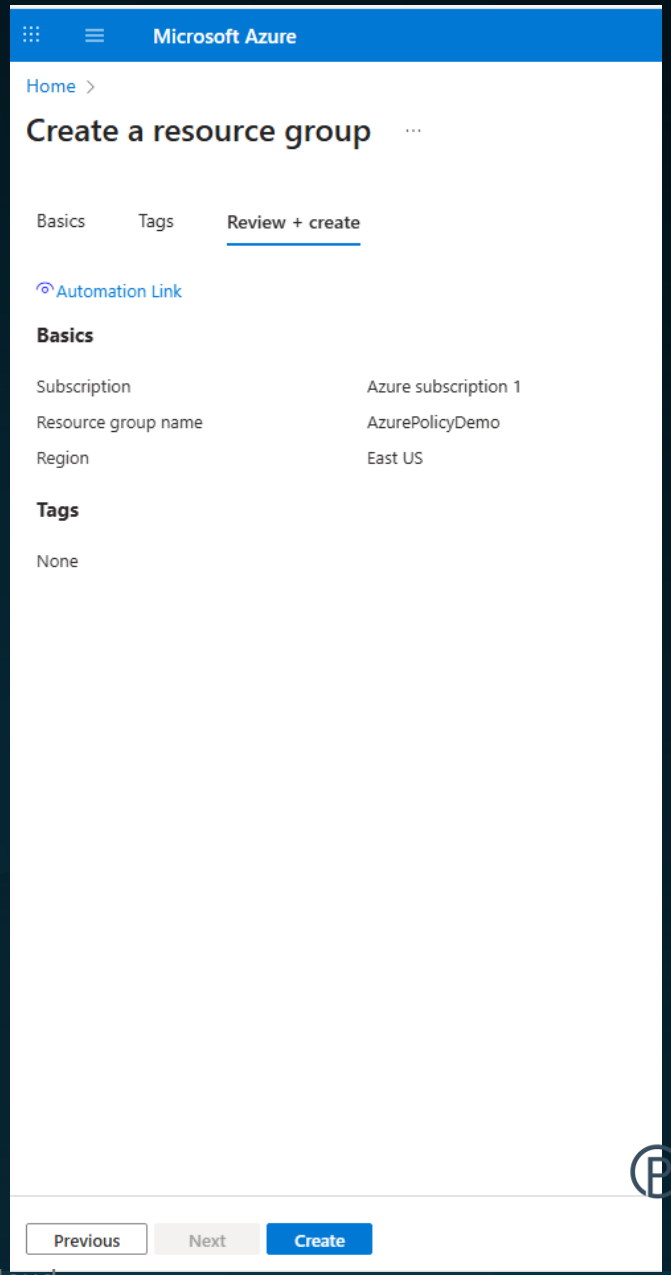
Why Azure Policy Matters (Architect View)

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**



PerparimLabs

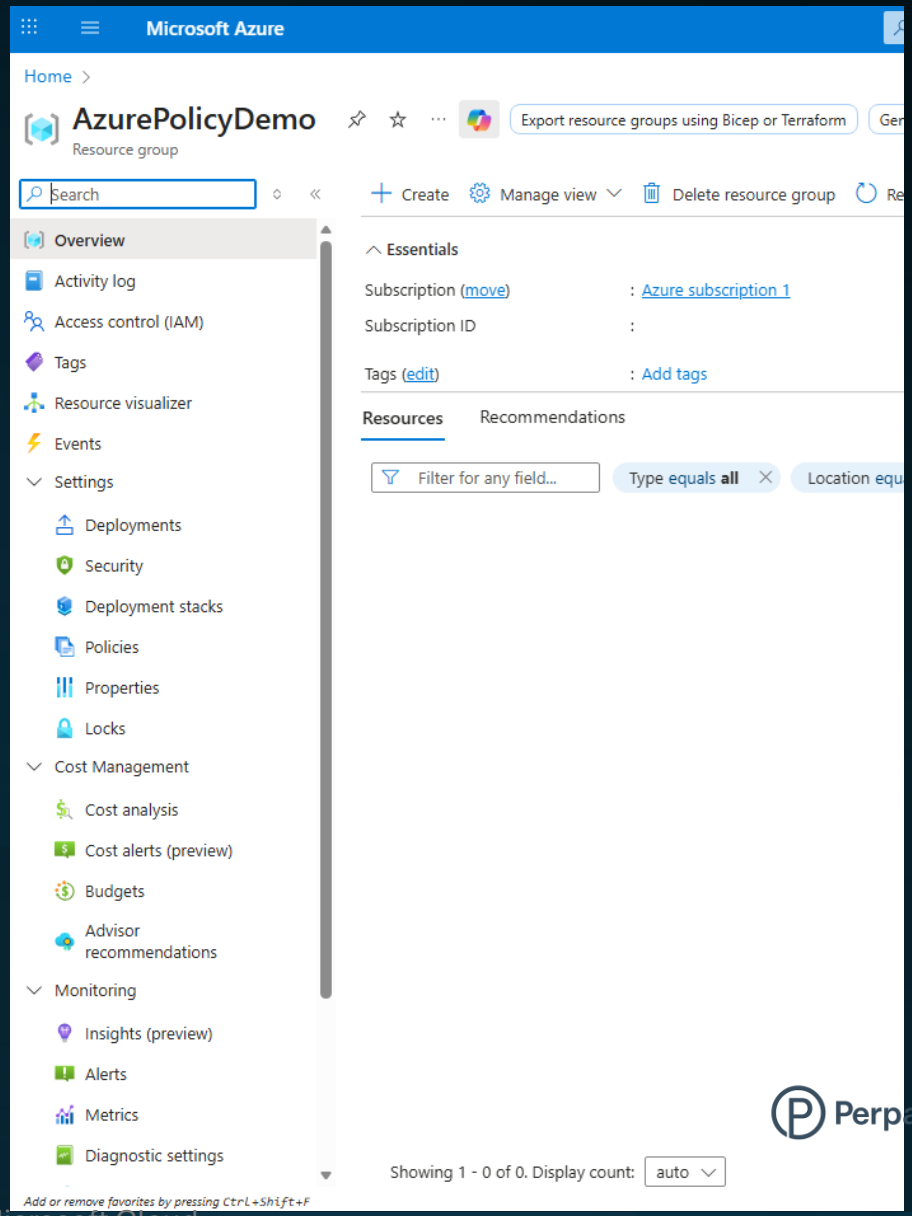
Create a Dedicated Resource Group

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.

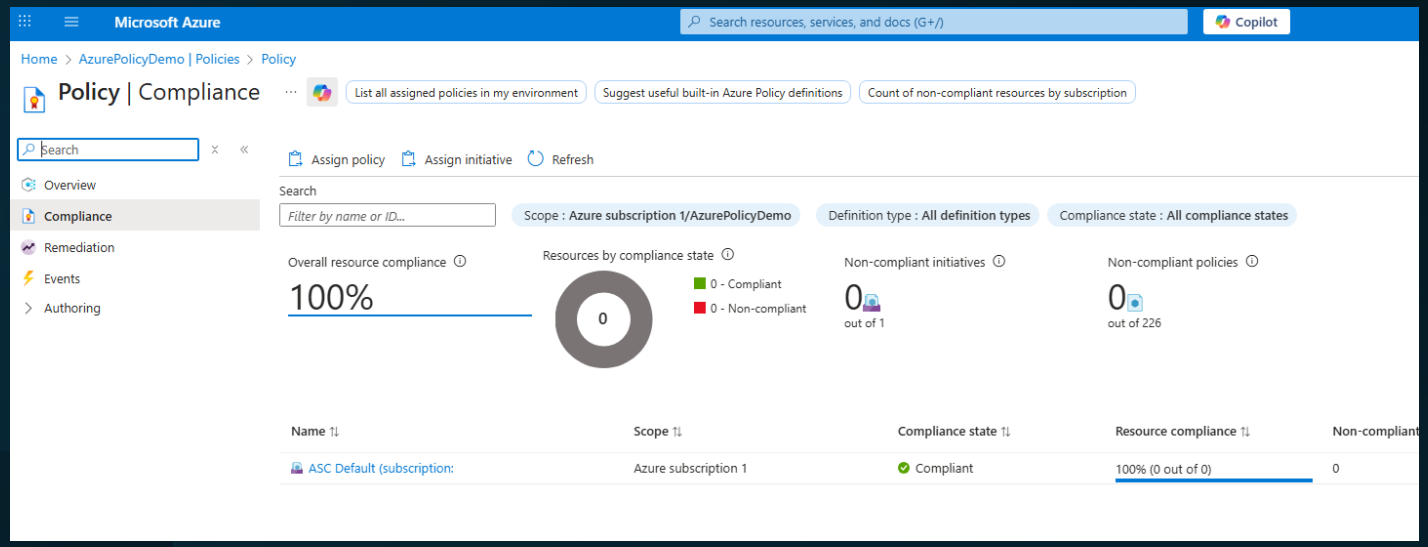


Azure Policy Compliance Dashboard

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.



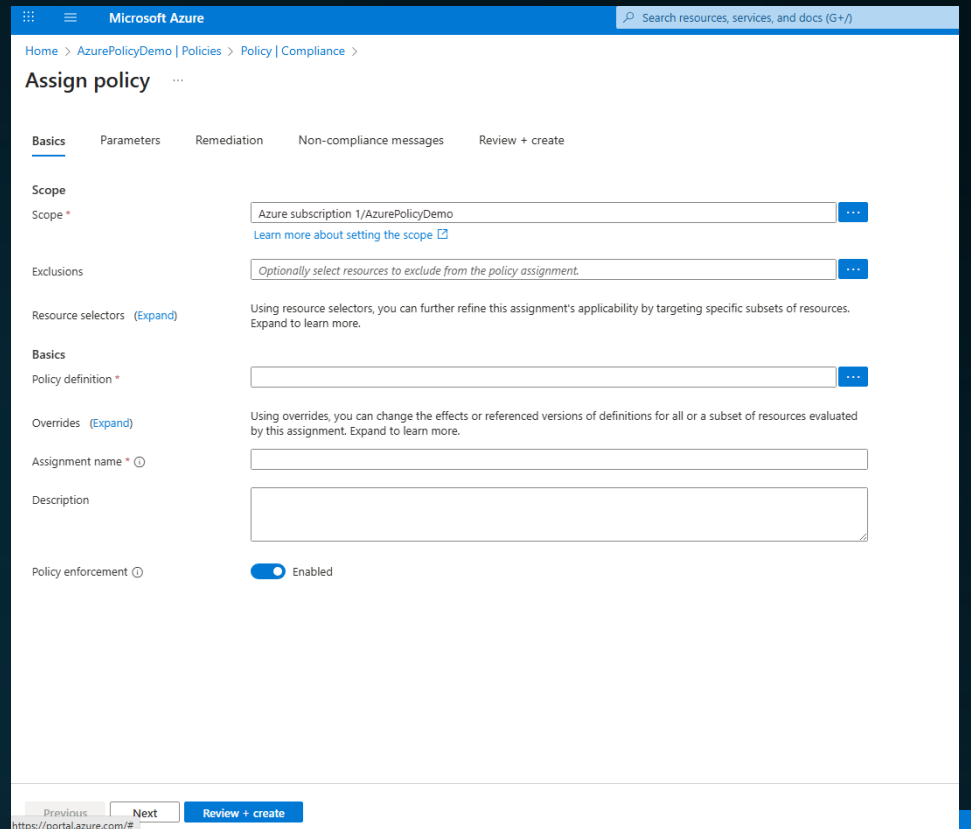
Assign a New Policy

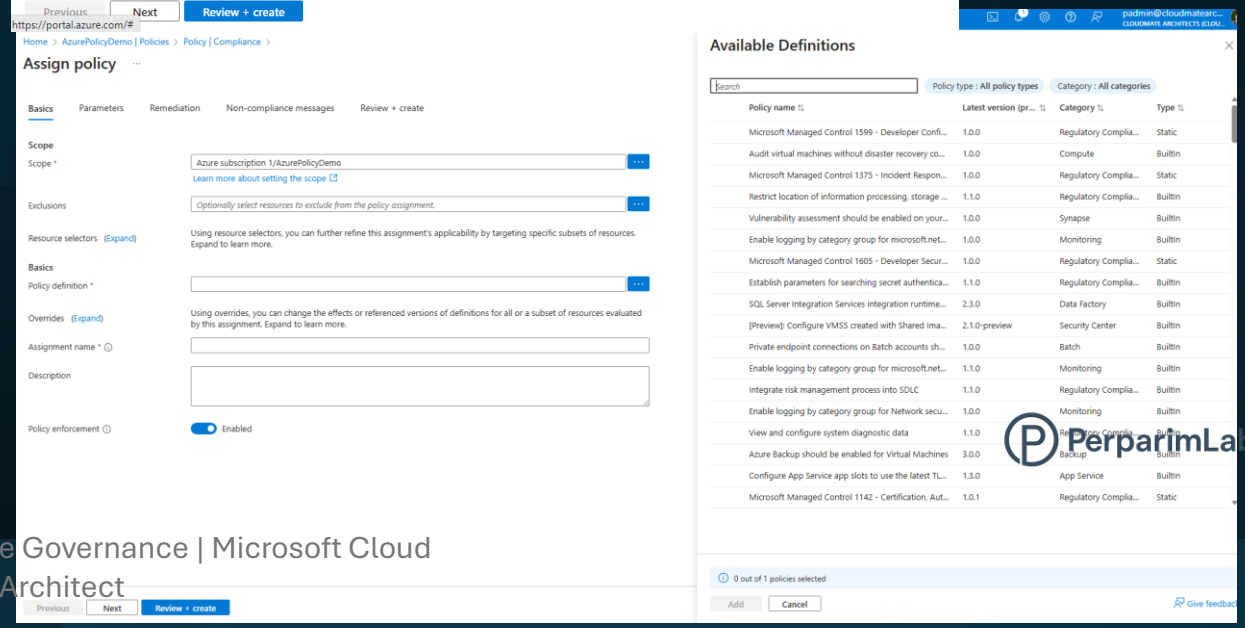
Navigate to:
Resource Group → **Policies** → *Assign policy*.

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.





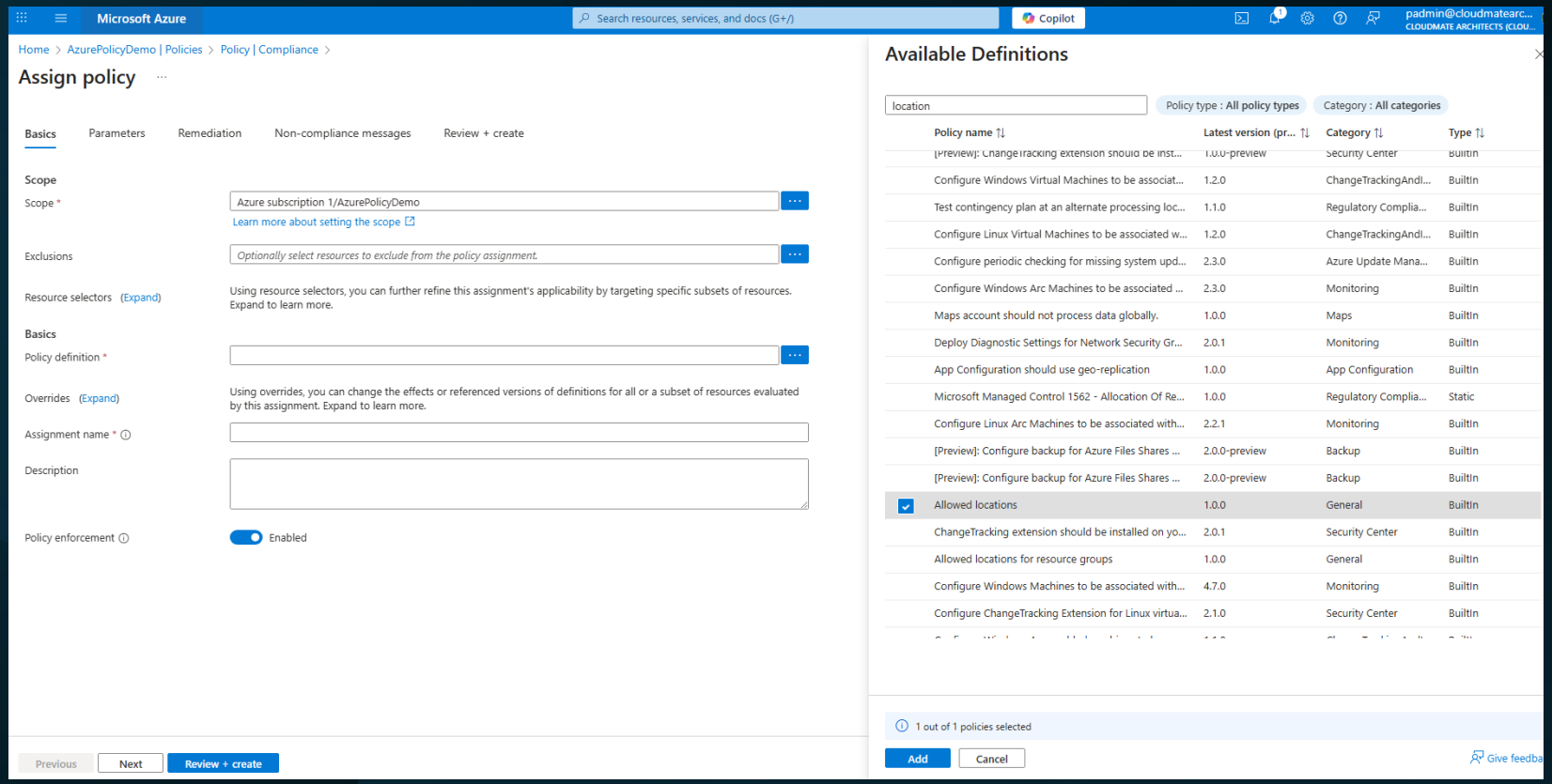
Select the Policy Definition

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.

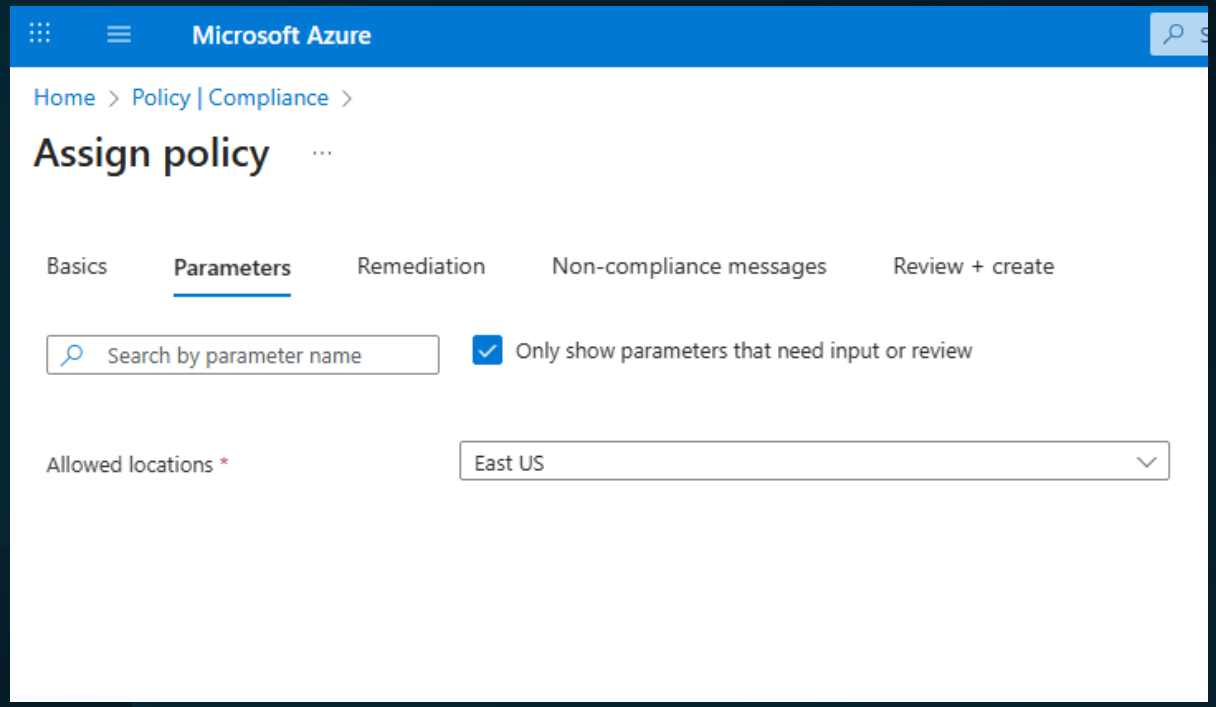


Configure the Policy Parameters

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.



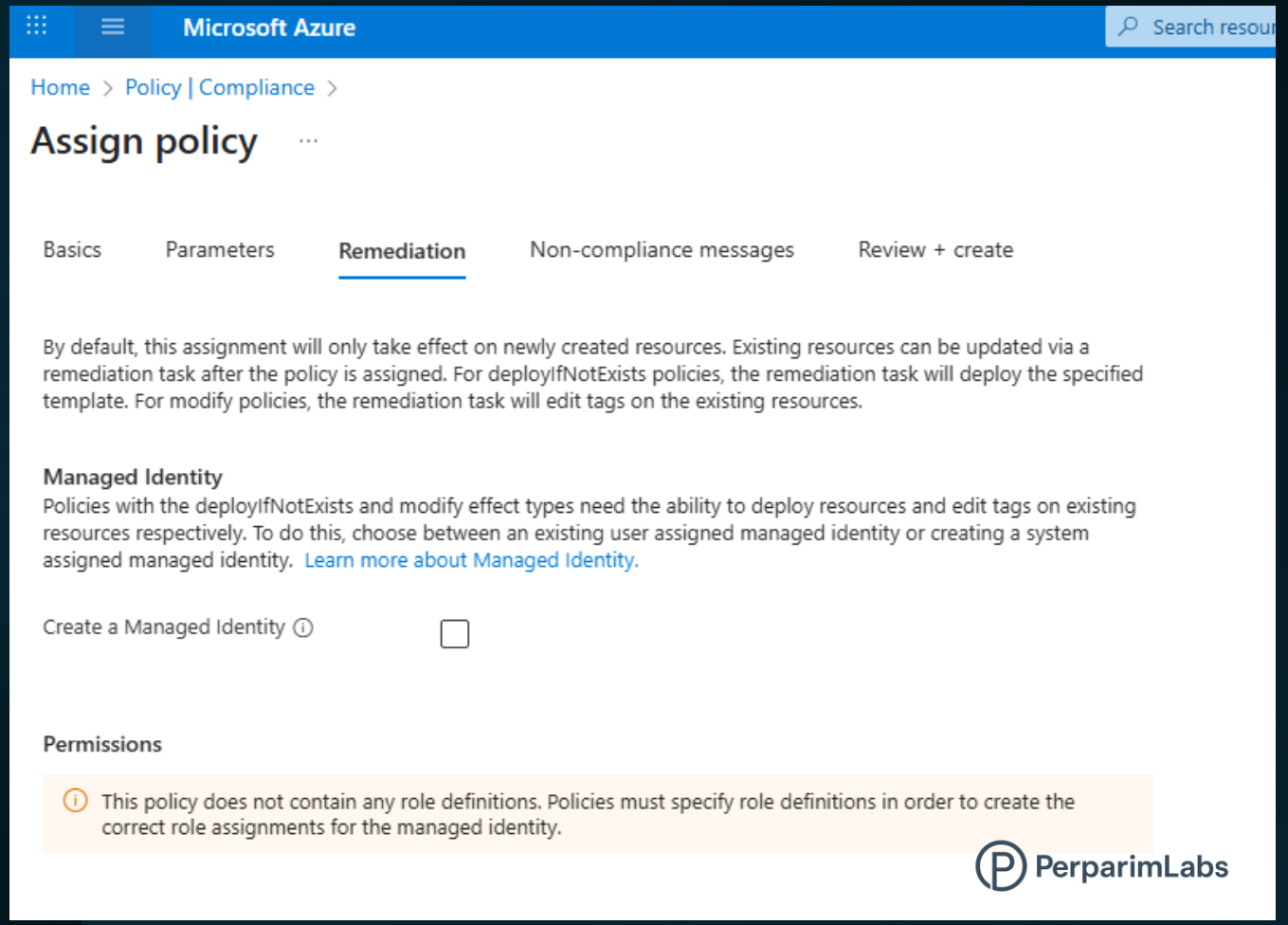
PerparimLabs

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.

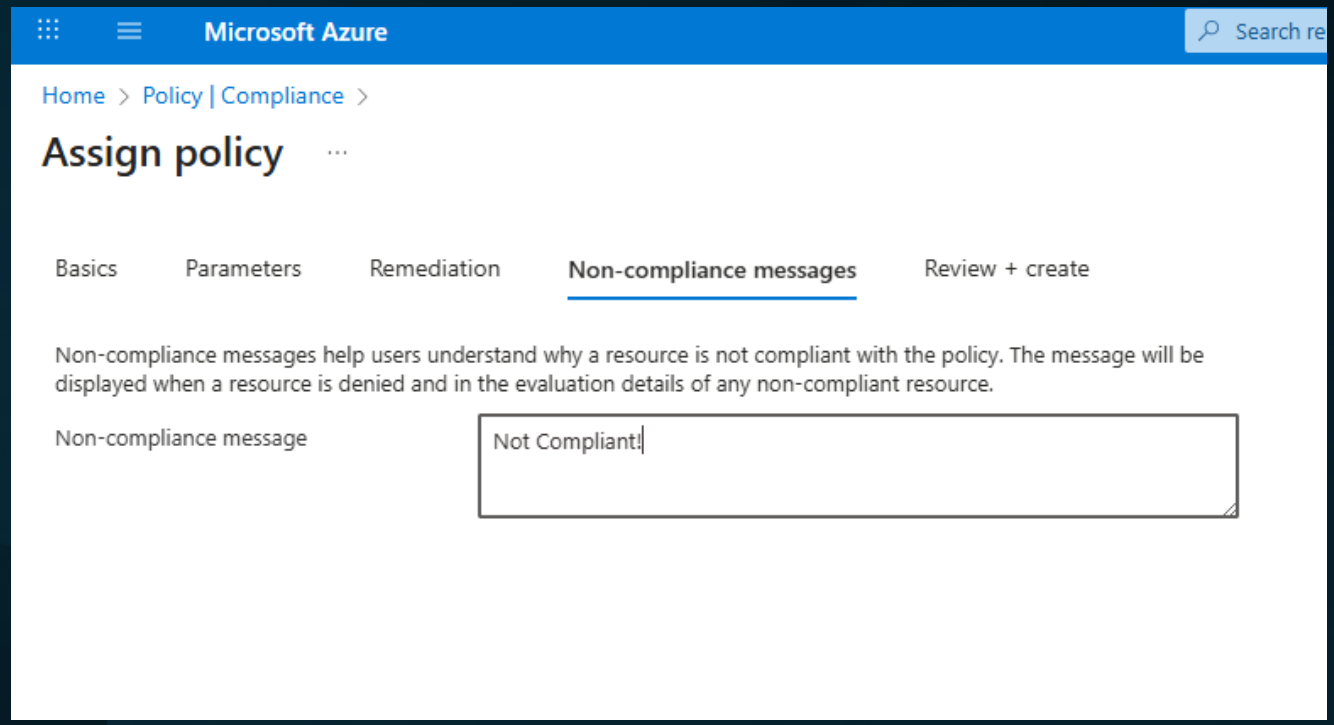


Non-Compliance Message

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

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

This improves DevOps feedback loops.



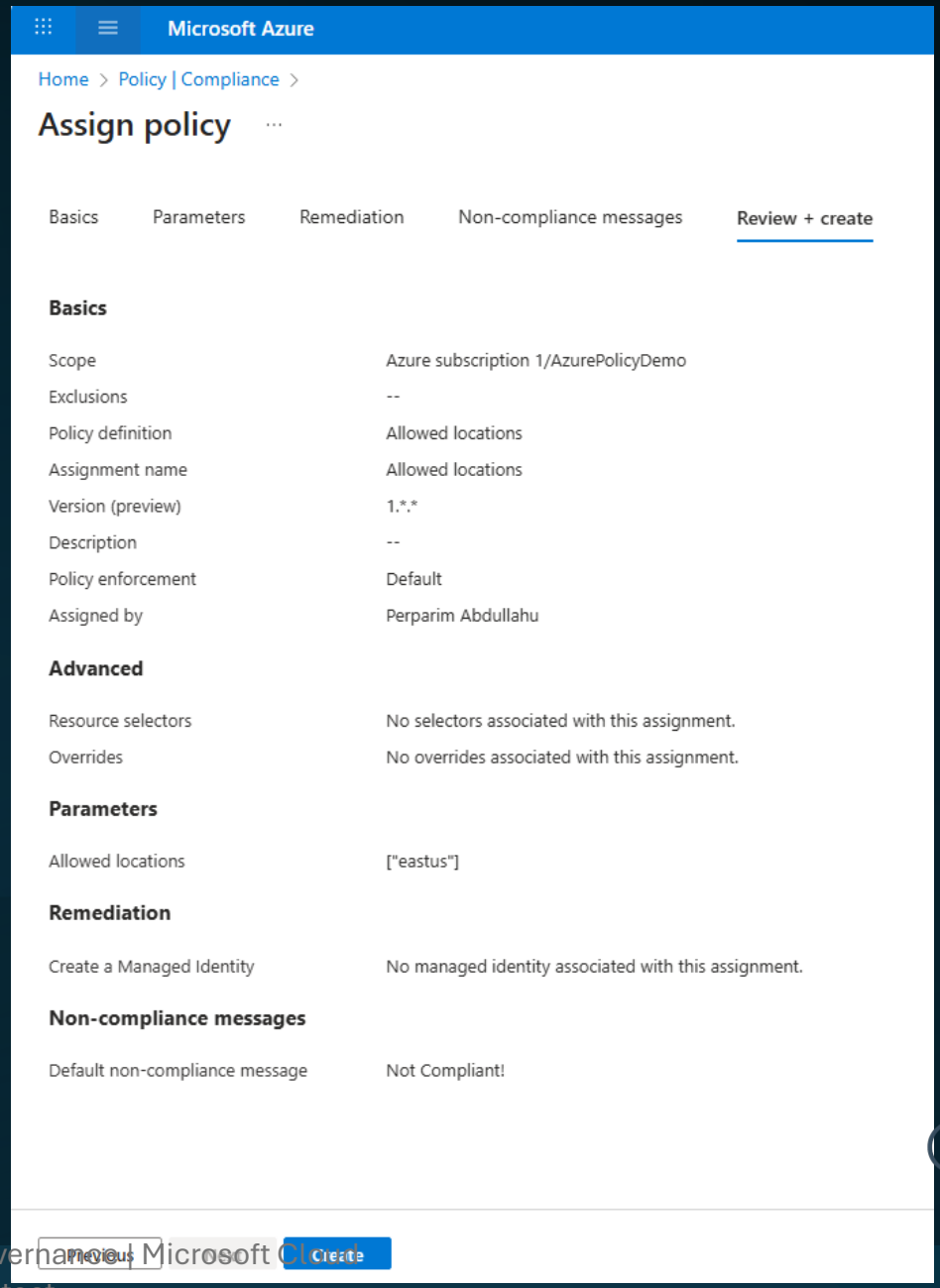
PerparimLabs

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.

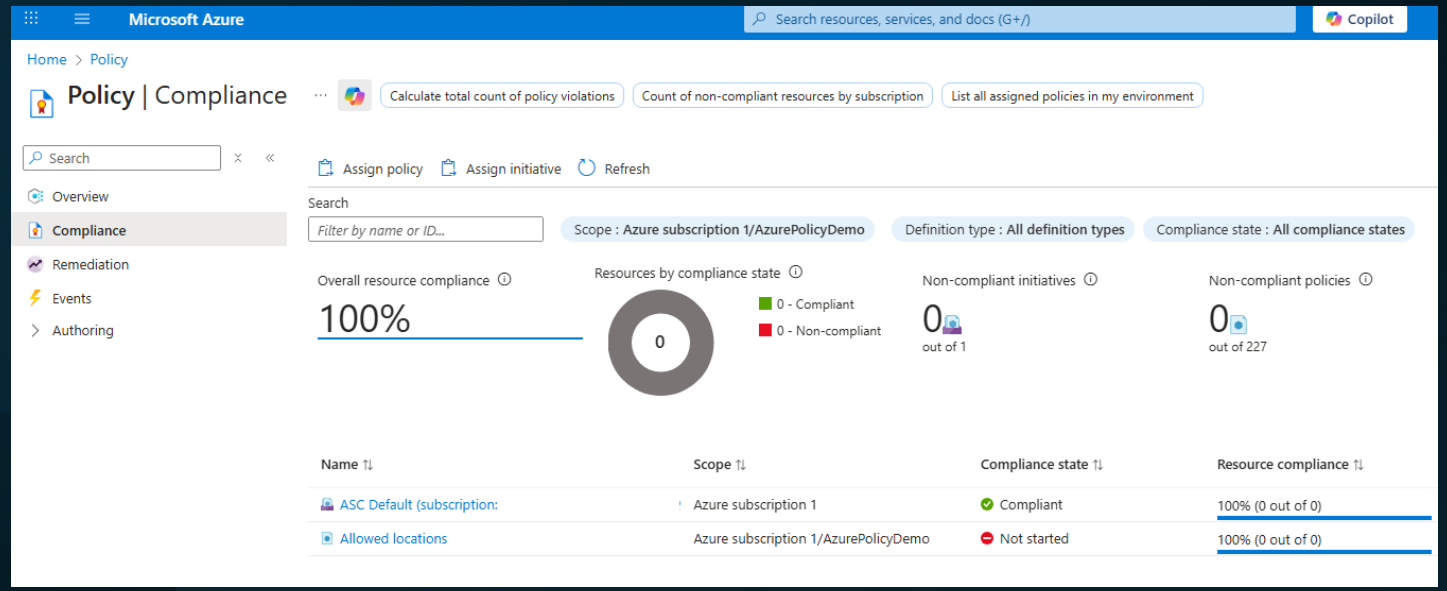


Compliance Evaluation

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.

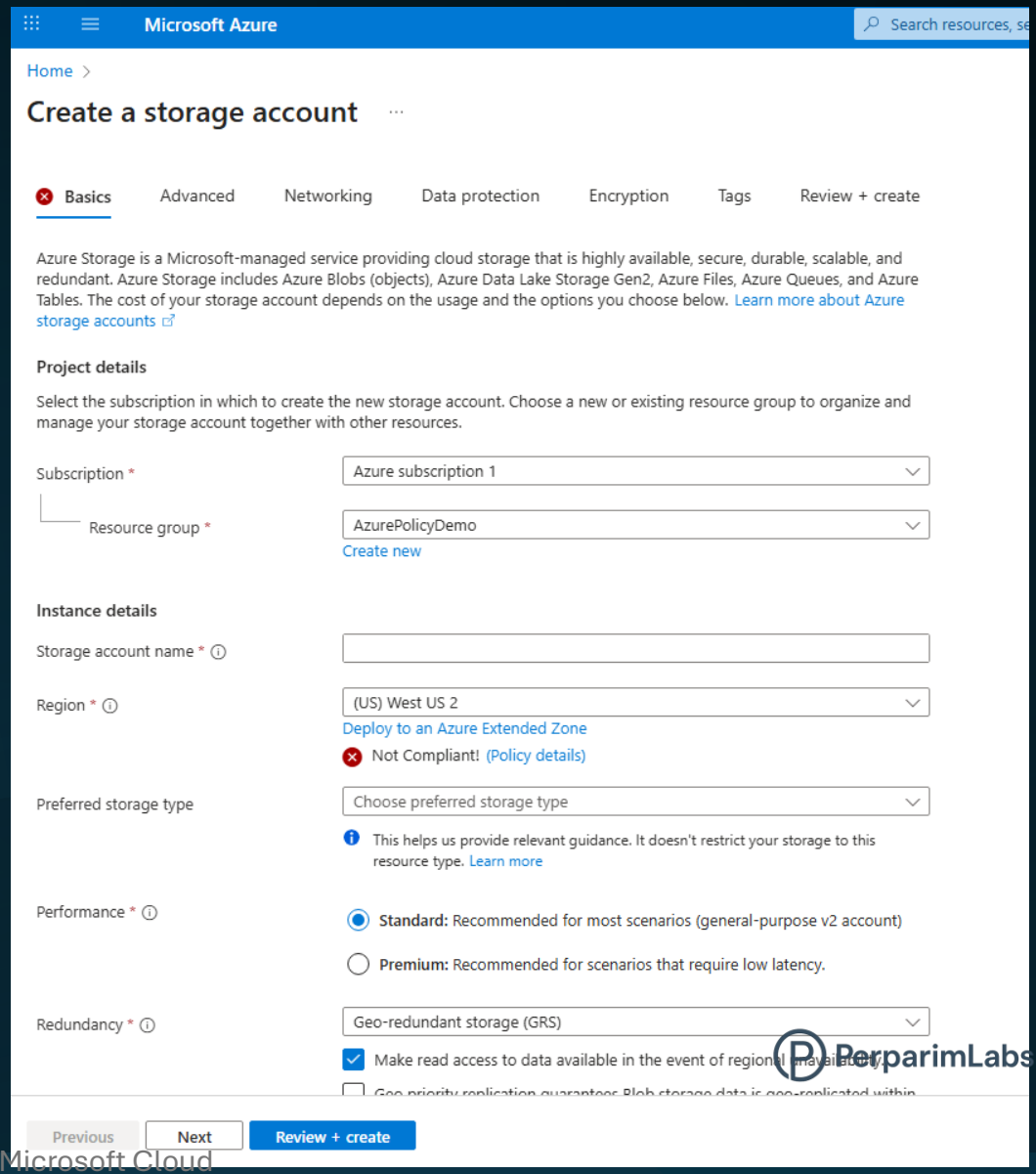
Example:

Region: **West US 2**

Policy applies → Azure immediately blocks the deployment

Error: **Not Compliant!**

This proves the policy is actively enforcing governance.



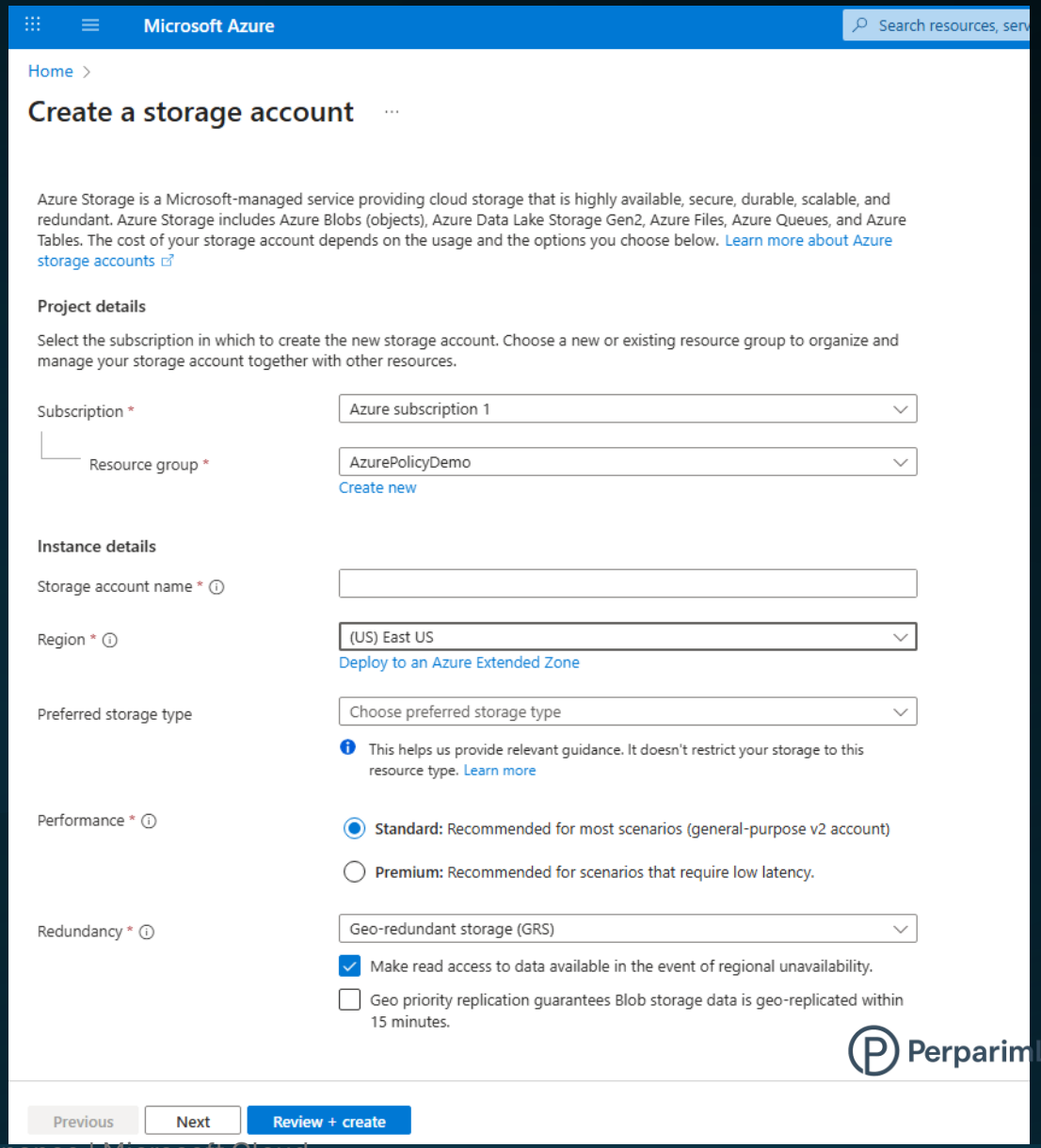
Test the Policy Again (Success Case)

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.



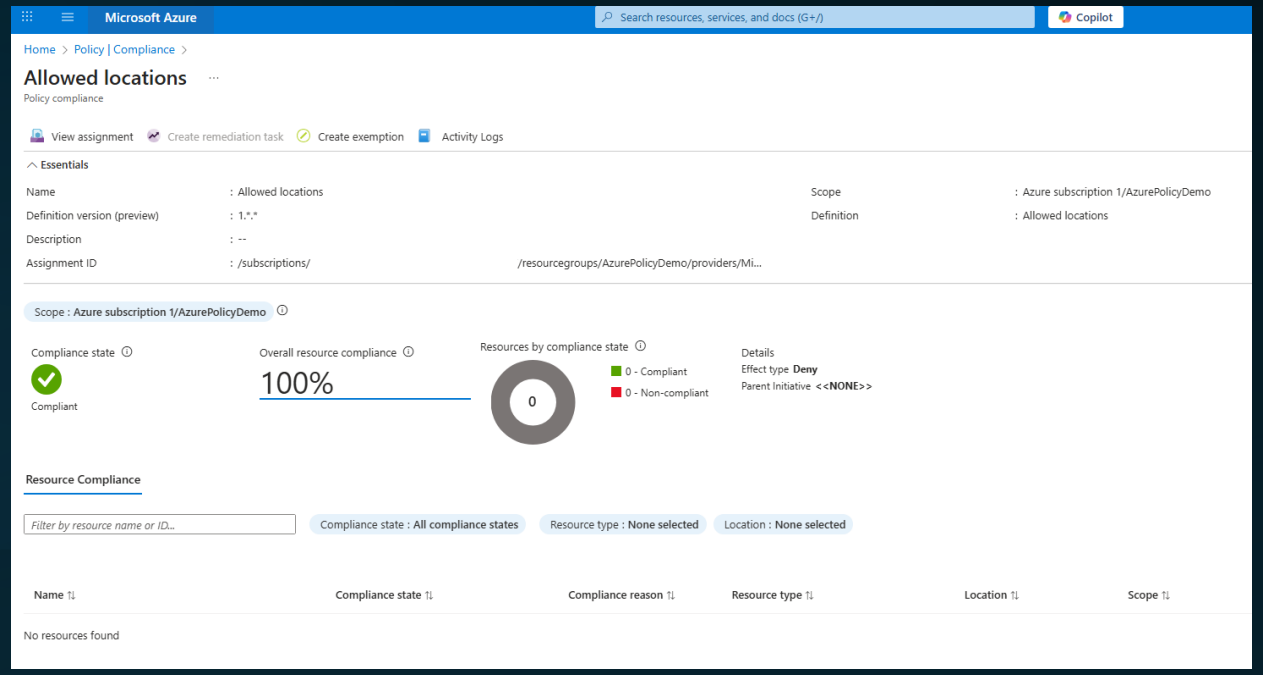
Policy Compliance Dashboard (After Enforcement)

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.