



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)

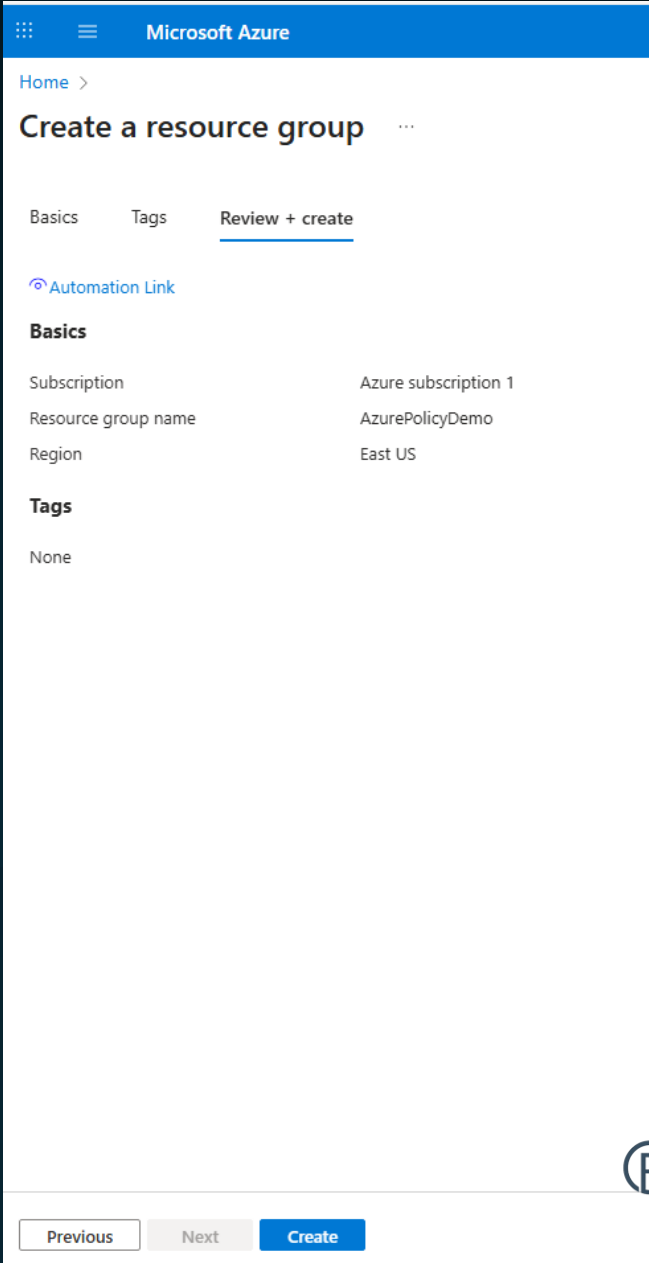
Azure Policy allows architects to **enforce organizational standards** and **prevent drift** across all cloud resources.

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**



The screenshot shows the Microsoft Azure portal interface for creating a new resource group. The top navigation bar is blue with the 'Microsoft Azure' logo. Below it, a breadcrumb trail shows 'Home >'. The main heading is 'Create a resource group' with a three-dot menu icon. There are three tabs: 'Basics', 'Tags', and 'Review + create', with the last one being the active tab. A link for 'Automation Link' is visible. Under the 'Basics' section, the following details are shown: Subscription is 'Azure subscription 1', Resource group name is 'AzurePolicyDemo', and Region is 'East US'. Under the 'Tags' section, the value is 'None'. At the bottom, there are three buttons: 'Previous' (disabled), 'Next' (disabled), and 'Create' (active).

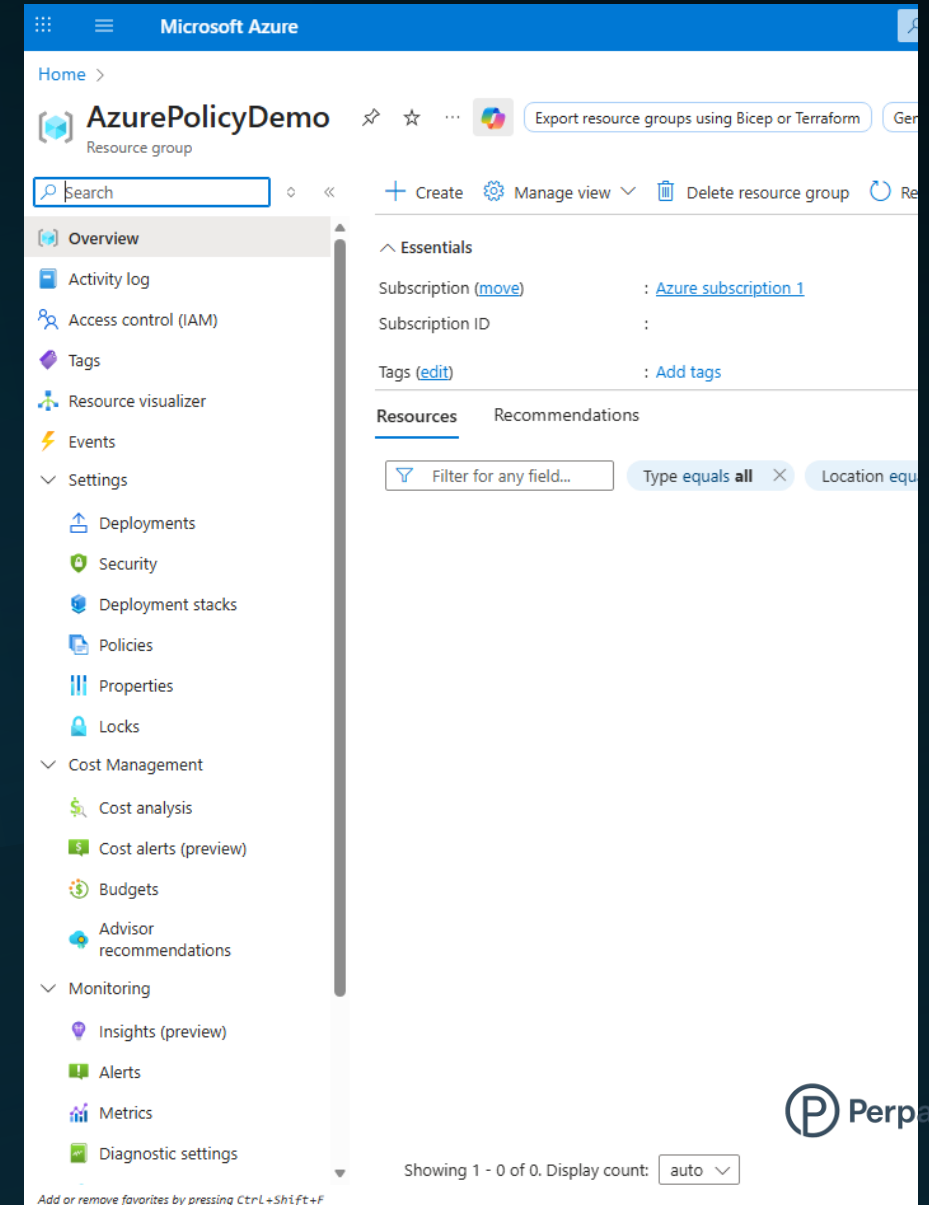
Create a Dedicated Resource Group

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.



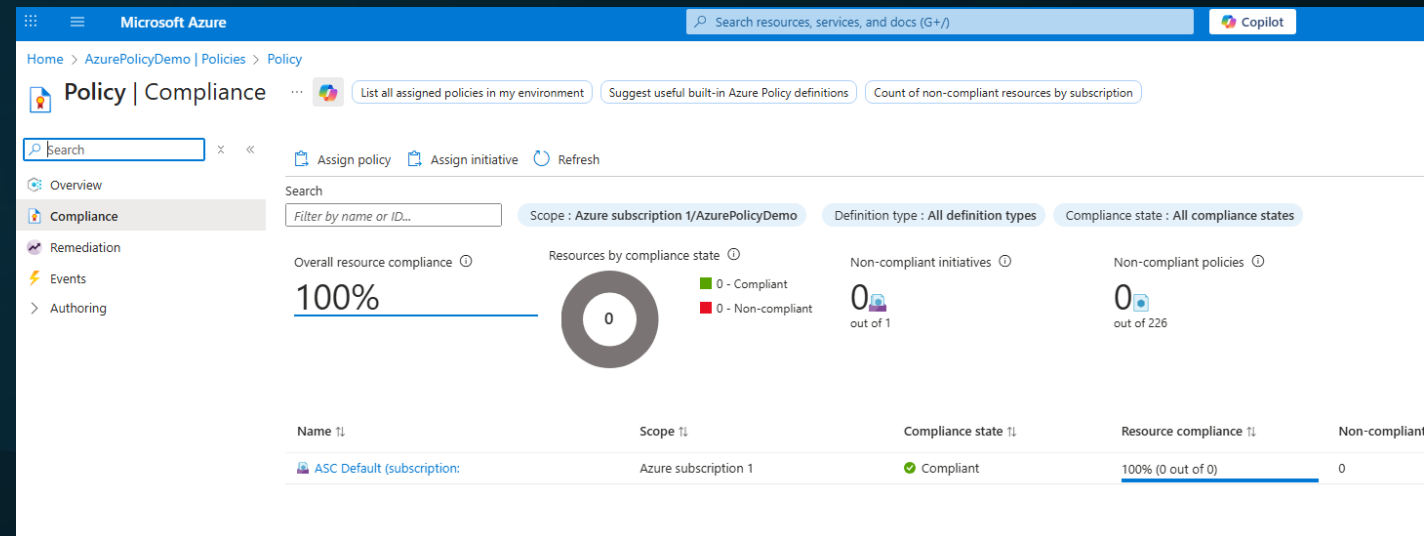
Azure Policy Compliance Dashboard

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.

The screenshot displays the Microsoft Azure portal interface for assigning a new policy. The top navigation bar shows the path: Home > AzurePolicyDemo | Policies > Policy | Compliance > Assign policy. The main content area is divided into tabs: Basics, Parameters, Remediation, Non-compliance messages, and Review + create. The 'Basics' tab is active, showing fields for Scope, Exclusions, Resource selectors, Policy definition, Overrides, Assignment name, and Description. The 'Scope' field is set to 'Azure subscription 1/AzurePolicyDemo'. The 'Policy definition' field is empty. The 'Assignment name' field is empty. The 'Policy enforcement' toggle is set to 'Enabled'. The 'Available Definitions' panel is open on the right, showing a list of policy definitions with columns for Policy name, Latest version, Category, and Type. The list includes various Microsoft Managed Controls and built-in policies.

Microsoft Azure

Home > AzurePolicyDemo | Policies > Policy | Compliance > Assign policy

Basics Parameters Remediation Non-compliance messages Review + create

Scope

Scope *

Exclusions

Resource selectors (Expand)

Basics

Policy definition *

Overrides (Expand)

Assignment name *

Description

Policy enforcement ☒ Enabled

Previous Next Review + create

Available Definitions

Policy name	Latest version	Category	Type
Microsoft Managed Control 1599 - Developer Conf...	1.0.0	Regulatory Compl...	Static
Audit virtual machines without disaster recovery co...	1.0.0	Compute	Built-in
Microsoft Managed Control 1375 - Incident Respon...	1.0.0	Regulatory Compl...	Static
Restrict location of information processing, storage ...	1.1.0	Regulatory Compl...	Built-in
Vulnerability assessment should be enabled on your...	1.0.0	Synapse	Built-in
Enable logging by category group for microsoft.net...	1.0.0	Monitoring	Built-in
Microsoft Managed Control 1605 - Developer Secur...	1.0.0	Regulatory Compl...	Static
Establish parameters for searching secret authentica...	1.1.0	Regulatory Compl...	Built-in
SQL Server Integration Services integration runtime...	2.3.0	Data Factory	Built-in
[Preview] Configure VMSS created with Shared ima...	2.1.0-preview	Security Center	Built-in
Private endpoint connections on Batch accounts sh...	1.0.0	Batch	Built-in
Enable logging by category group for microsoft.net...	1.1.0	Monitoring	Built-in
Integrate risk management process into SDLC	1.1.0	Regulatory Compl...	Built-in
Enable logging by category group for Network secu...	1.0.0	Monitoring	Built-in
View and configure system diagnostic data	1.1.0	Regulatory Compl...	Built-in
Azure Backup should be enabled for Virtual Machines	3.0.0	Backup	Built-in
Configure App Service app slots to use the latest TL...	1.3.0	App Service	Built-in
Microsoft Managed Control 1142 - Certification, Aut...	1.0.1	Regulatory Compl...	Static

0 out of 1 policies selected

Add Cancel

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 displays the Microsoft Azure portal interface for assigning a policy. The main section is titled 'Assign policy' and includes tabs for 'Basics', 'Parameters', 'Remediation', 'Non-compliance messages', and 'Review + create'. The 'Basics' tab is active, showing fields for 'Scope' (set to 'Azure subscription 1/AzurePolicyDemo'), 'Exclusions' (set to 'Optionally select resources to exclude from the policy assignment'), 'Resource selectors' (expanded), 'Policy definition' (empty), 'Overrides' (expanded), 'Assignment name' (empty), 'Description' (empty), and 'Policy enforcement' (set to 'Enabled').

On the right side, the 'Available Definitions' panel is open, showing a list of policy definitions. The search filter is set to 'location'. The table below lists the available definitions:

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

At the bottom of the 'Available Definitions' panel, it shows '1 out of 1 policies selected' and buttons for 'Add' and 'Cancel'.

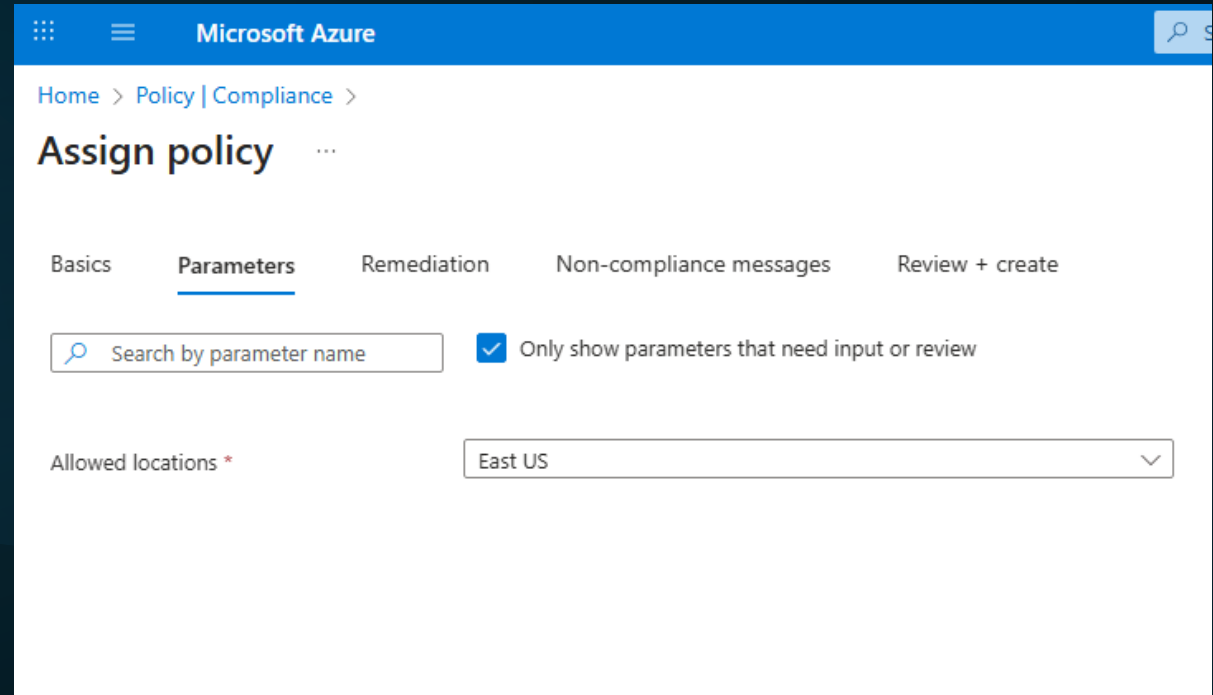
Configure the Policy Parameters

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.



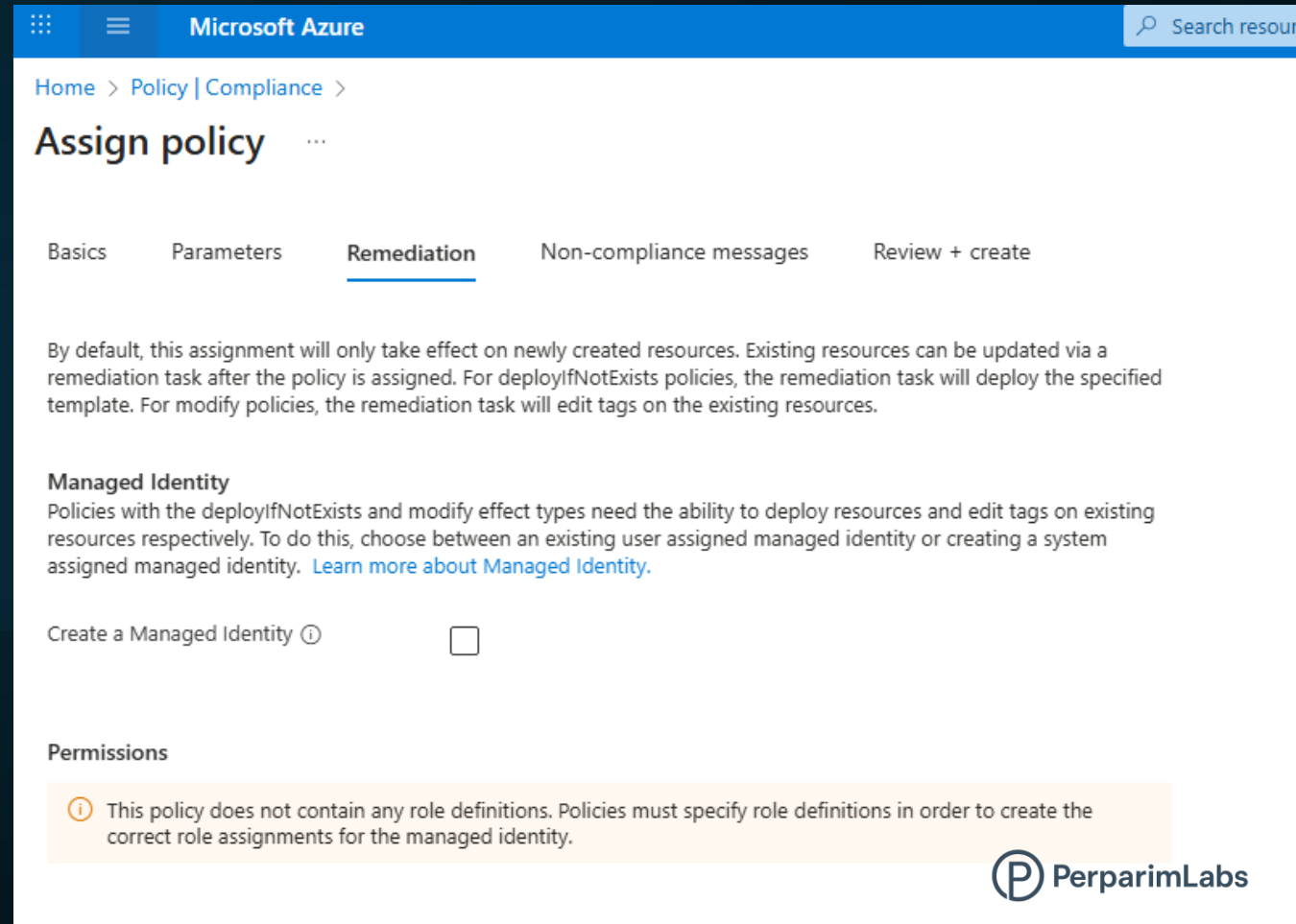
The screenshot shows the 'Assign policy' page in the Microsoft Azure portal, specifically the 'Parameters' tab. The page has a blue header with the 'Microsoft Azure' logo and a search icon. Below the header, there is a breadcrumb trail: 'Home > Policy | Compliance >'. The main heading is 'Assign policy' with a three-dot menu icon. There are five tabs: 'Basics', 'Parameters' (which is selected and underlined), 'Remediation', 'Non-compliance messages', and 'Review + create'. Below the tabs, there is a search bar labeled 'Search by parameter name' with a magnifying glass icon. To the right of the search bar is a checkbox labeled 'Only show parameters that need input or review', which is checked. Below this, there is a label 'Allowed locations *' followed by a dropdown menu showing 'East US' with a downward arrow.

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 'Assign policy' page in the Microsoft Azure portal, specifically the 'Remediation' tab. The page has a blue header with the 'Microsoft Azure' logo and a search bar. Below the header, there's a breadcrumb trail: 'Home > Policy | Compliance >'. The main heading is 'Assign policy' with a three-dot menu icon. There are five tabs: 'Basics', 'Parameters', 'Remediation' (which is selected and underlined), 'Non-compliance messages', and 'Review + create'. The 'Remediation' tab content explains that by default, the assignment only takes effect on newly created resources. It also mentions that existing resources can be updated via a remediation task after the policy is assigned. Below this, there's a section titled 'Managed Identity' which states that policies with 'deployIfNotExists' and 'modify' effect types need the ability to deploy resources and edit tags. It advises choosing between an existing user assigned managed identity or creating a system assigned managed identity, with a link to 'Learn more about Managed Identity'. There is a checkbox labeled 'Create a Managed Identity' with an information icon. At the bottom, there's a 'Permissions' section with a warning message: '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 PerparimLabs logo is in the bottom right corner.

Microsoft Azure

Home > Policy | Compliance >

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.


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 ⓘ ☐

Permissions

ⓘ 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.

 PerparimLabs

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.

Microsoft Azure

Home > Policy | Compliance >

Assign policy

Basics Parameters Remediation Non-compliance messages Review + create

Non-compliance messages help users understand why a resource is not compliant with the policy. The message will be displayed when a resource is denied and in the evaluation details of any non-compliant resource.

Non-compliance message

Not Compliant!

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.

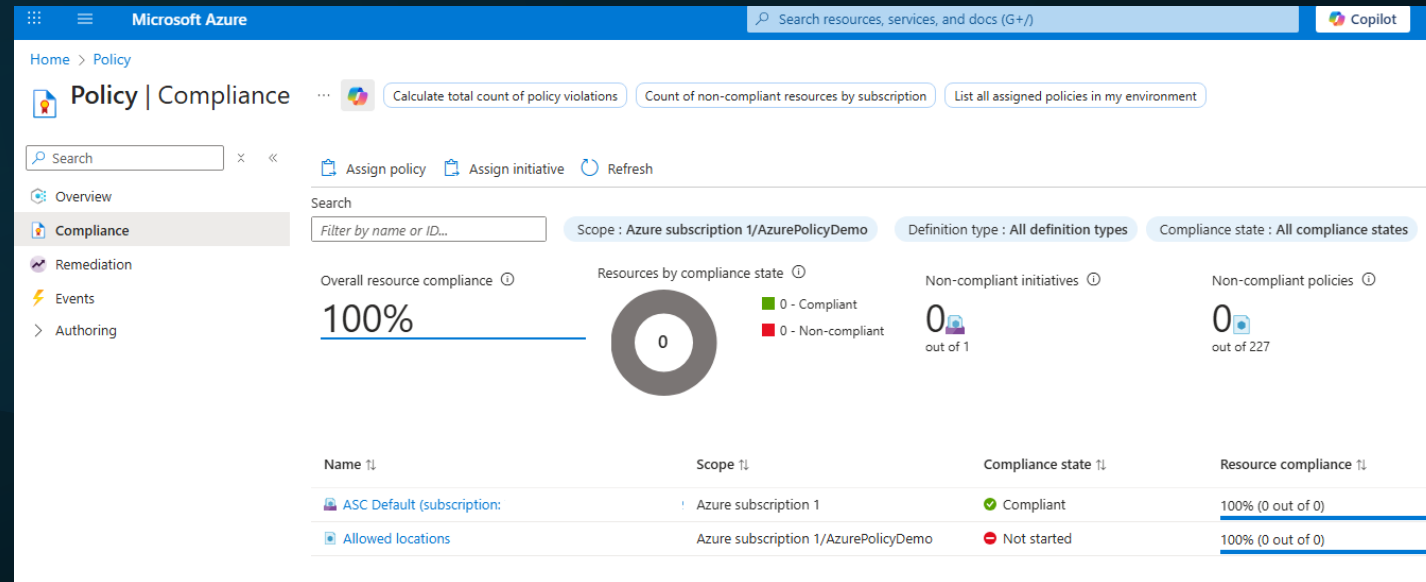
The screenshot shows the 'Assign policy' page in the Microsoft Azure portal, specifically the 'Review + create' tab. The page is divided into sections: Basics, Advanced, Parameters, Remediation, and Non-compliance messages. The 'Basics' section contains fields for Scope, Exclusions, Policy definition, Assignment name, Version (preview), Description, Policy enforcement, and Assigned by. The 'Advanced' section contains fields for Resource selectors and Overrides. The 'Parameters' section contains a field for Allowed locations. The 'Remediation' section contains a field for Create a Managed Identity. The 'Non-compliance messages' section contains a field for Default non-compliance message. At the bottom of the page, there are buttons for 'Previous', 'Cancel', and 'Create'.

Microsoft Azure	
Home > Policy Compliance >	
Assign policy ...	
Basics Parameters Remediation Non-compliance messages <u>Review + create</u>	
Basics	
Scope	Azure subscription 1/AzurePolicyDemo
Exclusions	--
Policy definition	Allowed locations
Assignment name	Allowed locations
Version (preview)	1.*
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!
Previous Cancel 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.

Microsoft Azure

Home >

Create a storage account

Basics Advanced Networking Data protection Encryption Tags Review + create

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
[Create new](#)

Instance details

Storage account name * ①

Region * ① (US) West US 2
[Deploy to an Azure Extended Zone](#)
✗ Not Compliant! [\(Policy details\)](#)

Preferred storage type Choose preferred storage type

① This helps us provide relevant guidance. It doesn't restrict your storage to this resource type. [Learn more](#)

Performance * ①

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

☐ Premium: Recommended for scenarios that require low latency.

Redundancy * ①

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

Previous Next Review + create

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
[Create new](#)

Instance details

Storage account name *

Region * (US) East US
[Deploy to an Azure Extended Zone](#)

Preferred storage type Choose preferred storage type

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

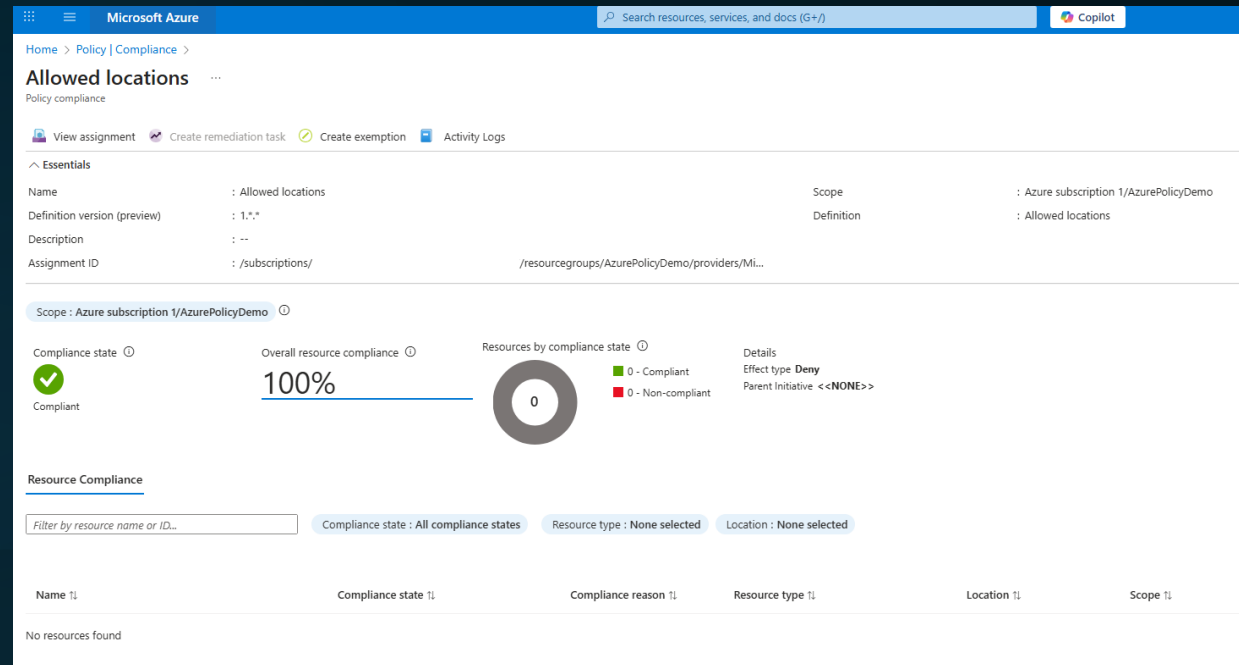
Policy Compliance Dashboard (After Enforcement)

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.

