THOMAS MORE

Lab 5.3

Azure Policy Guardrails

Toepasbare Cloud Security voor IT-Professionals

2025 - 2026

Contents

1. Azure Policy Guardrails

1.1. Context

In Labs 5.1 and 5.2, you observed compliance violations in your Day 5 deployment and manually improved the environment.

Manual fixes are useful for learning, but they do not scale. If every team has to remember every governance rule, mistakes will return.

In this lab, you will use Azure Policy as a guardrail mechanism. You will review built-in policy definitions, assign policies to your lab resource group, and test how Azure Policy affects new or updated resources.

This lab focuses on prevention and visibility:

- `Deny` policies can block non-compliant create or update operations.
- `Audit` policies can report non-compliance without blocking the operation.
- Existing resources can be shown as non-compliant.
- Existing resources are not automatically fixed by `Deny` or `Audit`.

> **Note**
>
> Azure Policy is one mechanism for enforcing governance at scale in Azure. Built-in policies are maintained by Microsoft. Custom policies are used when an organization needs rules that are specific to its own standards.

1.2. Learning goals

By the end of this lab, you should be able to explain:

- What an Azure Policy definition is.
- What an Azure Policy assignment is.
- How policy scope affects enforcement.
- The difference between `Audit` and `Deny`.
- Why policy compliance and policy enforcement are related but not identical.
- Why existing non-compliant resources may require remediation in a later lab.

1.3. Estimated time

45 minutes

Suggested timing:

Time	Activity
10 minutes	Review built-in policy definitions
10 minutes	Assign a required tag policy
10 minutes	Assign or review a storage public access policy
10 minutes	Test policy enforcement and compliance
5 minutes	Reflection and discussion

1.4. Before you start

Make sure you have:

- [ ] Day 5 infrastructure deployed.
- [ ] Lab 5.2 manual fixes completed or reviewed.
- [ ] Access to the Azure portal.
- [ ] Permission to assign policy at the lab resource group scope.

> **Note**
>
> Assigning Azure Policy requires permission to create policy assignments at the selected scope. Owner and Resource Policy Contributor are common roles for this. Plain Contributor is usually not enough to assign policies, although it can manage many resources.

2. Azure Policy Concepts

Before assigning policies, review the basic concepts.

Concept	Meaning
Policy definition	The rule. It describes what condition is checked and what effect is applied.
Policy assignment	The act of applying a policy definition to a scope.
Scope	Where the policy applies: management group, subscription, resource group, or resource.
Effect	What Azure Policy does when the rule matches, such as `Audit` or `Deny`.
Compliance state	Whether existing resources in scope match the policy rules.

2.1. Common effects

Effect	Meaning
`Audit`	Allows the request but records non-compliance. Useful for visibility and reporting.
`Deny`	Blocks matching create or update requests. Useful for hard guardrails.
`Modify`	Can add, update, or remove supported properties or tags. Useful for safe automatic correction.
`DeployIfNotExists`	Can deploy related configuration when it is missing, such as diagnostic settings.

> **Note**
>
> This lab focuses mainly on `Audit` and `Deny`. Lab 5.5 focuses on remediation, where `Modify` and `DeployIfNotExists` become important.

3. Review Built-in Policies

Azure Policy has many built-in definitions. In this lab, you will inspect policies related to tags and storage account exposure.

3.1. Navigate to Azure Policy

1. In the Azure portal, search for **Policy**.
2. Open **Definitions**.
3. Use the search and category filters to find policies related to:
   - tags
   - storage accounts
   - public network access

> **Note**
>
> Built-in policy names, versions, and allowed effects can change. Always inspect the policy details and parameters in the portal instead of relying only on the title.

3.2. Review a required tag policy

Search for:

```
Require a tag and its value on resources
```

Open the policy definition and inspect:

- The description.
- The policy rule.
- The parameters.
- The available effect.

This policy is useful when every resource must include a specific tag and value, such as:

```
environment = dev
```

> **Note**
>
> A required tag policy is a good guardrail, but it does not automatically design a good tagging strategy. The organization must still decide which tags are required and which values are allowed.

3.3. Review a storage public access policy

Search for:

```
Storage accounts should disable public network access
```

or search more broadly for:

```
storage public network access
```

Open a relevant built-in policy and inspect:

- What condition it checks.
- Whether the effect is fixed or parameterized.
- Whether the policy audits or denies non-compliant storage accounts.
- Whether it checks public network access, blob public access, or another related storage setting.

> **Note**
>
> Storage account exposure has several related settings. `Public network access`, firewall rules, private endpoints, and blob anonymous access are different concepts. Read the selected policy carefully so you know exactly what it checks.

4. Assign a Required Tag Policy

Now assign a tag guardrail to your lab resource group.

4.1. Create the assignment

1. In the Policy blade, open **Assignments**.
2. Click **+ Assign policy**.
3. Set the scope to your Day 5 resource group.

Example:

`rg-<your_prefix>-d5`

4. Select the built-in policy:

`Require a tag and its value on resources`

5. Configure the parameters:

Parameter	Value
Tag name	`environment`
Tag value	`dev`

6. Make sure the assignment is enabled.
7. Review and create the assignment.

> **Note**
>
> If the portal asks for enforcement mode, keep enforcement enabled for this guardrail. Enforcement mode controls whether the policy effect is enforced during resource operations. Compliance evaluation can still occur separately.

4.2. Wait for compliance evaluation

After the assignment is created, compliance results may take several minutes to appear.

You can continue with the lab while waiting.

5. Test the Required Tag Guardrail

You will now test what happens when a new resource does not meet the tag requirement.

5.1. Try to create a resource without the required tag

Use the Azure portal or Azure CLI to create a small test resource in your lab resource group without the required `environment = dev` tag.

A simple option is to try creating a storage account. Storage account names must be globally unique and use only lowercase letters and numbers.

```
az storage account create `
  --name st<yourprefix>d5notag `
  --resource-group <RESOURCE_GROUP_NAME> `
  --location westeurope `
  --sku Standard_LRS
```

Expected result:

```
The create operation should fail if the required tag policy is enforced.
```

Now try again with the required tag:

```
az storage account create `
  --name st<yourprefix>d5tagged `
  --resource-group <RESOURCE_GROUP_NAME> `
  --location westeurope `
  --sku Standard_LRS `
  --tags environment=dev
```

Expected result:

```
The create operation should be allowed if the resource satisfies the policy.
```

> **Note**
>
> If the first command succeeds, check the assignment scope, enforcement mode, policy effect, and whether the selected policy applies to that resource type.

> **Question**
>
> What error or policy message do you see when creating a resource without the required tag?

6. Assign or Review a Storage Public Access Policy

Next, assign or review a policy related to storage account public network access.

> **Note**
>
> This part of the lab is about understanding storage guardrails. Depending on the selected built-in policy and its available effects, your instructor may ask you to use `Audit` first, then discuss when `Deny` is appropriate.

6.1. Create the assignment

1. In the Policy blade, open **Assignments**.
2. Click **+ Assign policy**.
3. Set the scope to your Day 5 resource group.
4. Select a built-in policy related to storage account public network access, such as:

```
Storage accounts should disable public network access
```

5. Inspect the parameters.
6. If the policy allows selecting an effect, choose one of the following based on the instructor's direction:

Effect	Use when
`Audit`	You want visibility first and do not want to block or break existing workflows.
`Deny`	You are confident that public network access should not be allowed in this lab scope.

7. Review and create the assignment.

6.2. Discuss the selected policy

Answer:

Your answer:

Which storage setting does your selected policy check?

Does it check public network access, blob anonymous access, firewall rules, or another setting?

Which effect did you choose, and why?

> **Note**
>
> A storage account can have public network access enabled without allowing anonymous public blob access. Public network access controls whether the storage account endpoint can be reached over public networks. Blob anonymous access controls whether blobs can be read anonymously when container permissions allow it.

7. Review the Policy Compliance Dashboard

7.1. Navigate to compliance

1. In the Policy blade, click **Compliance**.
2. Set the scope to your lab resource group.
3. Review the compliance state of your policy assignments.

Look for:

- The required tag policy.
- The storage public access policy.
- Any non-compliant resources.

> **Note**
> Policy compliance state can lag behind resource changes. If the portal does not update immediately, wait a few minutes. Your instructor may also trigger a policy evaluation scan.

7.2. Review non-compliant resources

Click a non-compliant policy result and inspect:

Which resource is non-compliant. Which policy assignment detected it. **Which effect is configured.** Whether the resource is existing or newly created.

> **Question**
> Why is the compliance dashboard more useful than checking each resource manually?

8. Existing Resources Versus New Changes

Azure Policy is often confusing because policy evaluation and policy enforcement are not the same thing.

Situation	What Azure Policy can show	What Azure Policy can do immediately
Existing non-compliant resource	Can appear as non-compliant after evaluation.	`Audit` and `Deny` do not automatically fix it.
New create request	Can be evaluated during the request.	`Deny` can block it.
Update to existing resource	Can be evaluated during the request.	`Deny` can block the update if the request violates the rule.
Remediable policy	Can show non-compliance.	`Modify` or `DeployIfNotExists` may be remediated through a remediation task.

> **Note**
>
> This is the bridge to Lab 5.5: guardrails can prevent future mistakes, but remediation tasks are needed when you want Azure Policy to fix supported existing violations.

9. Optional Cleanup of Test Resource

If you created a tagged test storage account, remove it unless your instructor wants to keep it for the next lab.

```
az storage account delete `
  --name st<yourprefix>d5tagged `
  --resource-group <RESOURCE_GROUP_NAME> `
  --yes
```

> **Note**
>
> Do not delete resources that are part of the Day 5 infrastructure unless instructed.

10. Reflection Questions

Your answer:

1. Which policies did you assign?
2. What happened when you tried to create a resource without the required tag?
3. What effect did your storage policy use: `Audit` or `Deny`?
4. What would happen if the same storage account were created in a different resource group outside the assignment scope?
5. Why does Azure Policy reduce reliance on manual checks?
6. Which existing violations still need remediation or manual review?

11. Summary

In this lab, you reviewed built-in Azure Policy definitions, assigned guardrails to your lab resource group, tested a required tag policy, and inspected policy compliance.

You learned that:

- Policy definitions describe rules.
- Policy assignments apply those rules to a scope.
- `Audit` creates visibility without blocking.
- `Deny` blocks non-compliant create or update operations.
- Existing non-compliant resources may still require manual fixes or remediation tasks.

Next, you will explore tags as an operational tool beyond compliance, and then use remediation tasks to fix supported policy violations automatically.