😊 Azure Policies

Azure Policies are a governance feature in Microsoft Azure that allow you to enforce rules and standards across your Azure resources. They provide a way to ensure compliance with organizational standards, regulatory requirements, and security policies. Azure Policies enable you to:

1. **Define Standards:** Specify rules and guidelines for resource configurations, such as naming conventions, resource types, tags, and allowed locations.
2. **Enforce Compliance:** Automatically evaluate and enforce compliance with defined policies, preventing deployments or configurations that violate policy rules.
3. **Ensure Security:** Enhance security posture by enforcing security controls, such as requiring encryption, network restrictions, or specific authentication mechanisms.
4. **Monitor and Remediate:** Continuously monitor resources for compliance with policies and automatically remediate non-compliant resources to bring them back into compliance.
5. **Centralize Governance:** Implement centralized governance across multiple subscriptions and resource groups, ensuring consistency and adherence to organizational standards.

The main goal of Azure Policies is to maintain a secure, compliant, and well-governed Azure environment by enforcing consistent rules and standards across all resources. They help organizations minimize risks, improve operational efficiency, and maintain regulatory compliance.

😄 Use cases of Azure Policies:

Azure Policies offer a wide range of use cases to enforce governance and compliance within Azure environments. Here are some common scenarios where Azure Policies are valuable:

1. **Resource Tagging:** Enforce tagging requirements for resources to ensure consistent tagging practices, which aids in resource organization, cost tracking, and resource management.
2. **Resource Configuration Standards:** Define and enforce configuration standards for Azure resources, such as requiring specific encryption settings, network configurations, or access controls.
3. **Compliance and Regulatory Requirements:** Ensure compliance with industry regulations (e.g., HIPAA, GDPR) or internal policies by enforcing specific security controls, data protection measures, or audit requirements.
4. **Cost Management:** Implement cost management policies to enforce budget limits, resource sizing guidelines, or the use of cost-effective resource types, helping to optimize cloud spending.

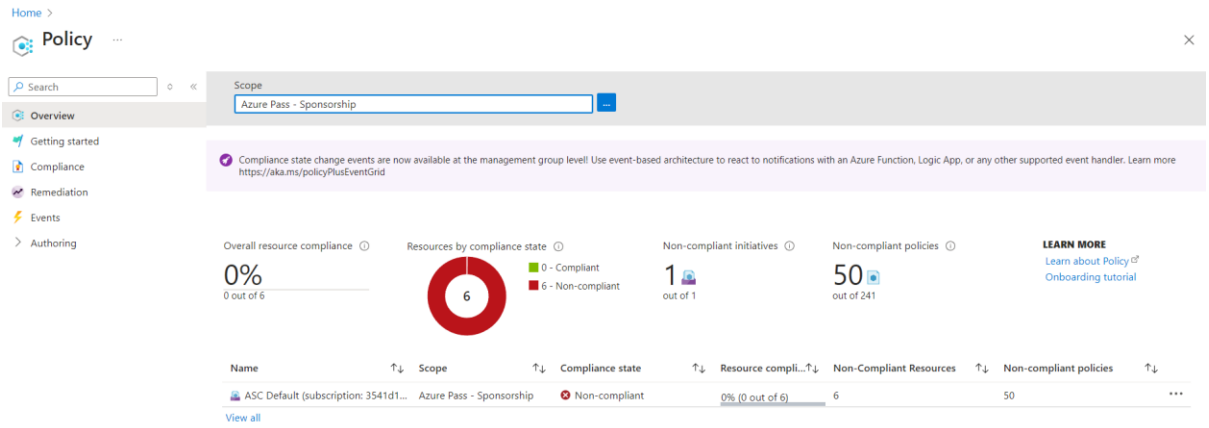
5. **Security Baselines:** Enforce security best practices and standards by requiring the use of specific security configurations, such as enabling Azure Security Center recommendations or enforcing network security groups.
6. **Access Control:** Control access to Azure resources by defining policies that restrict access based on user roles, permissions, or IP addresses, helping to prevent unauthorized access.
7. **Governance Across Subscriptions:** Establish consistent governance policies across multiple Azure subscriptions within an organization to ensure uniformity and adherence to organizational standards.
8. **Resource Lifecycle Management:** Define policies to govern the lifecycle of Azure resources, such as enforcing resource deletion after a specified period or requiring the use of specific resource deployment templates.
9. **Environment Segregation:** Implement policies to ensure segregation of environments (e.g., development, testing, production) by enforcing restrictions on resource deployments or configurations based on environment type.
10. **Service Level Agreements (SLAs):** Enforce SLA requirements by defining policies that ensure resources meet availability, performance, or reliability standards required by SLAs.

These use cases demonstrate the versatility of Azure Policies in enforcing governance, compliance, security, and cost management within Azure environments, helping organizations maintain a well-managed and secure cloud infrastructure.

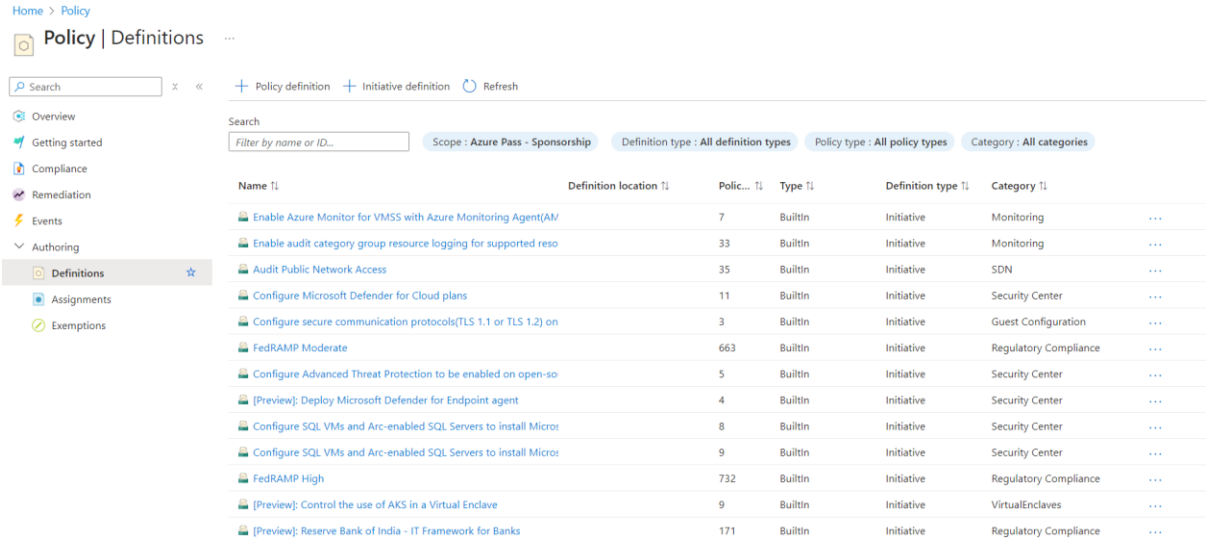
In this process, we are implementing and enforcing Azure policies to ensure resources are tagged correctly and to restrict the deployment of certain resource types. Initially, we configure a policy to require tags on all resources, then set up an automated remediation policy to add missing tags to non-compliant resources. Additionally, we create a policy to prevent the deployment of specific resource types, such as virtual machines, within designated resource groups. The end goal is to enhance resource management, maintain compliance with organizational standards, improve security, and streamline governance within the Azure environment.

😄 To begin with the Lab:

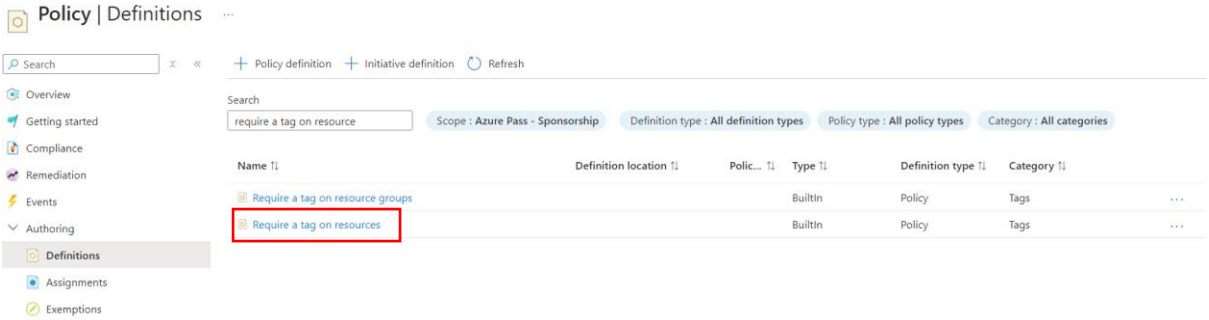
1. First you are going to remove the locks that we have placed in the earlier labs.
2. Now to start with this lab, first we need to search and navigate to policy.
3. This the dashboard of policy.



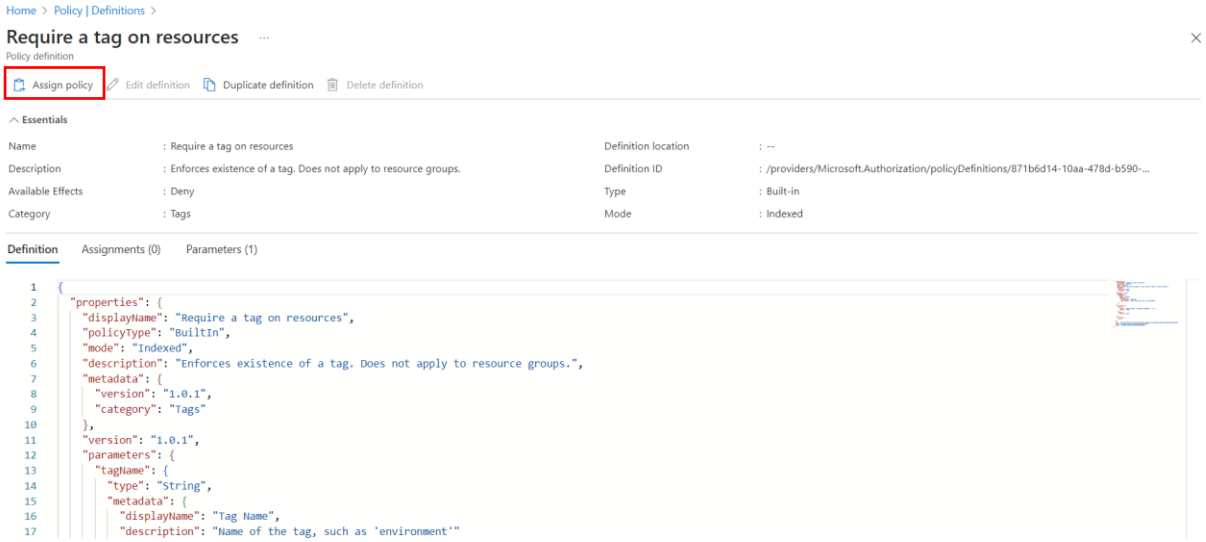
4. Now if you go to definitions then there you can see the various built in polices.



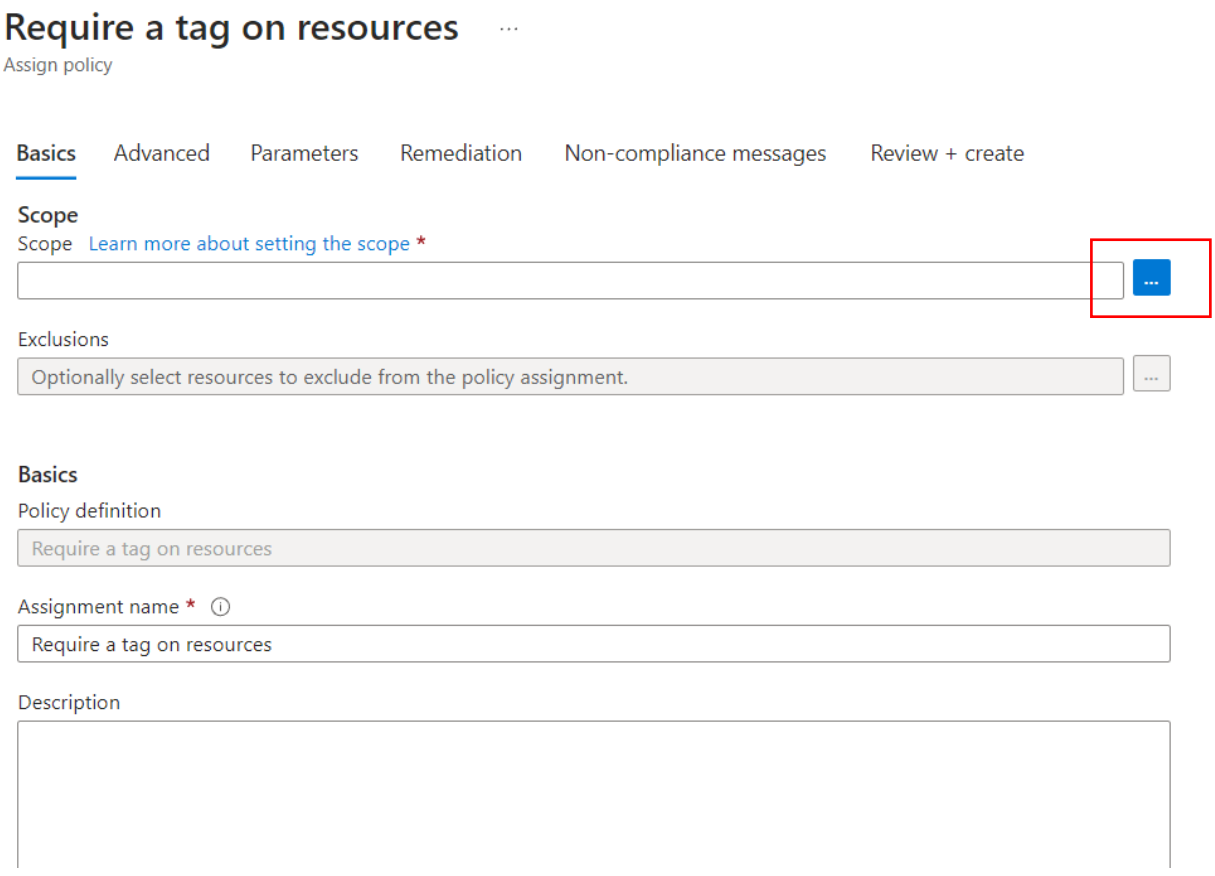
5. Then we need to search for the policy that says require a tag on resources. Click on it.



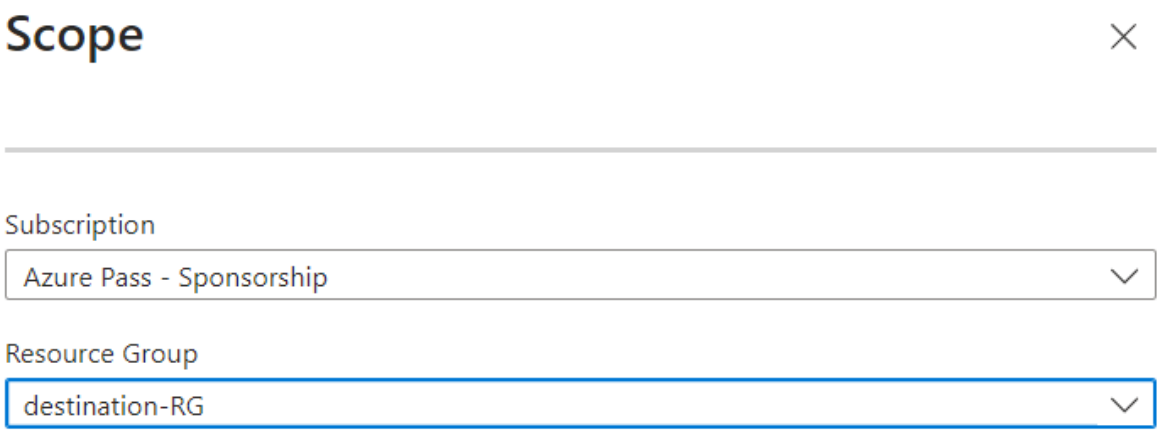
6. Then you can read about the policy. Now you need to click on Assign policy.



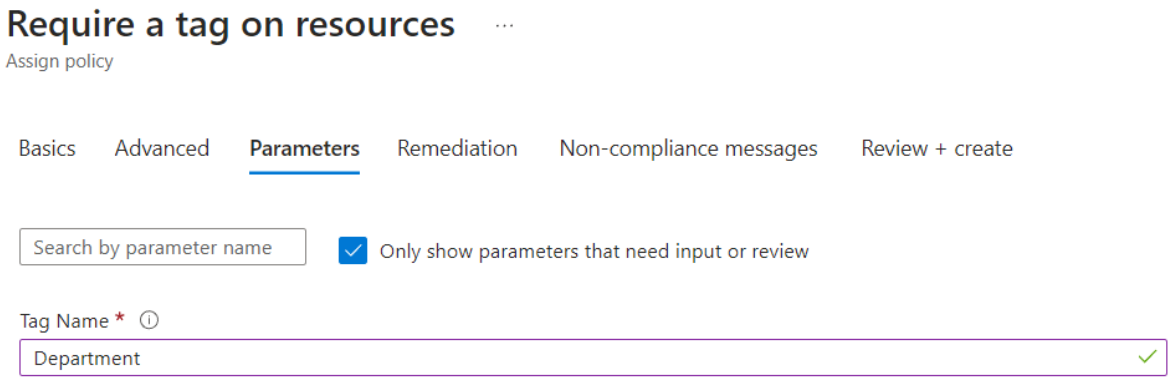
7. Now you will be on this page and here you need to click on the highlighted part.



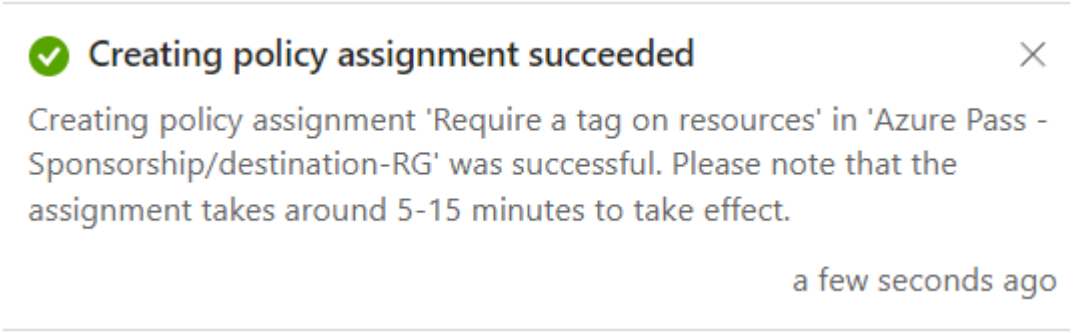
8. Then you have to choose your subscription and then choose the resource group.



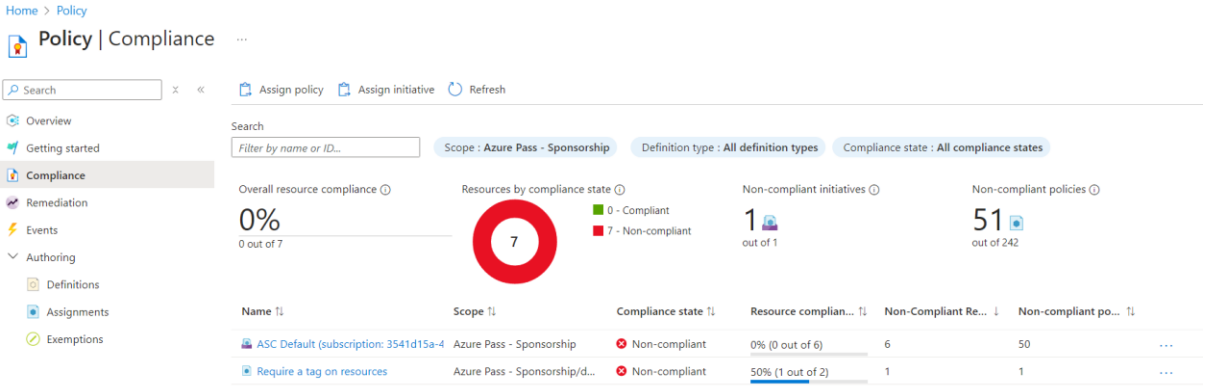
9. Now you need to move to parameters and describe your tag here.



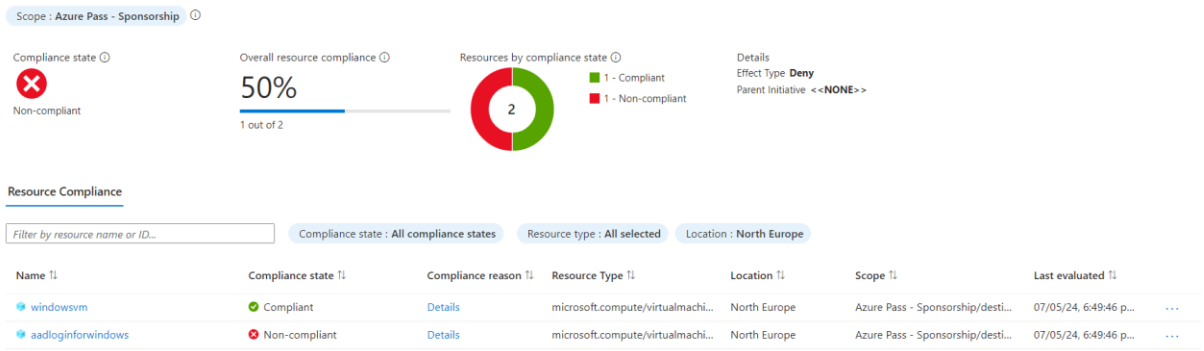
10. Then you will get this message that policy creation was successful. You can also see that it says it will take 5-15 minutes for this policy to take place.



11. Now if you go to Compliance in Policy then you can see that our policy was non-compliant.



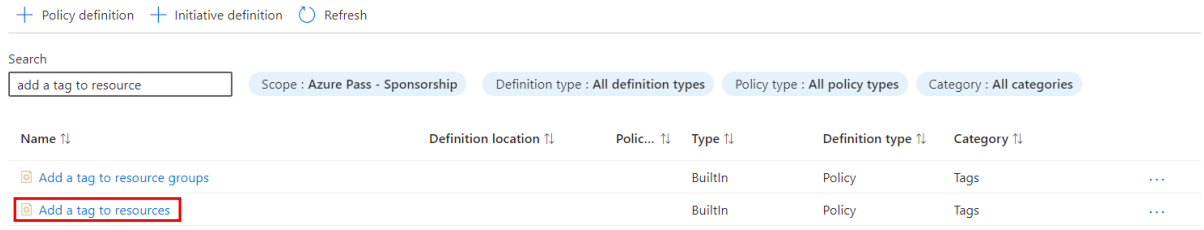
12. Now if you open your policy then you will see that it was fifty-fifty. Because your Windows VM has the tag on it but the add log does not that is why it went like that.



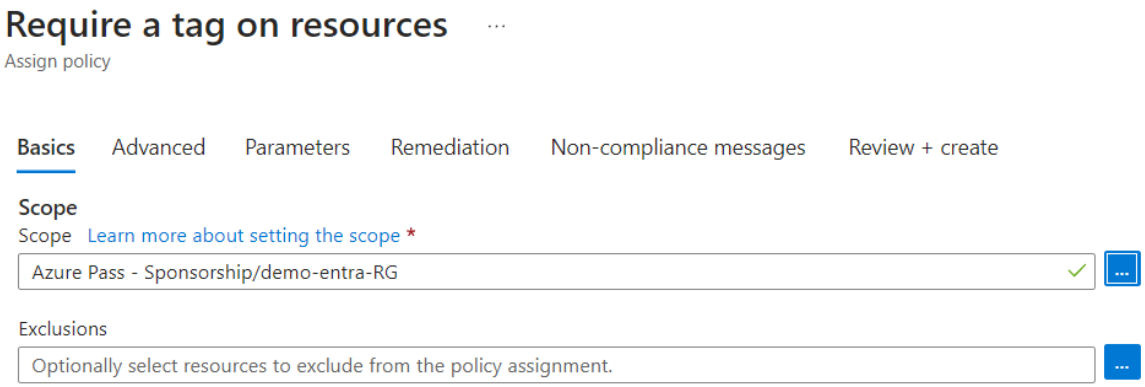
13. If in your resource group, there was only just your VM or this add log has the tag on it then your policy would've passed.

😄 Remediation

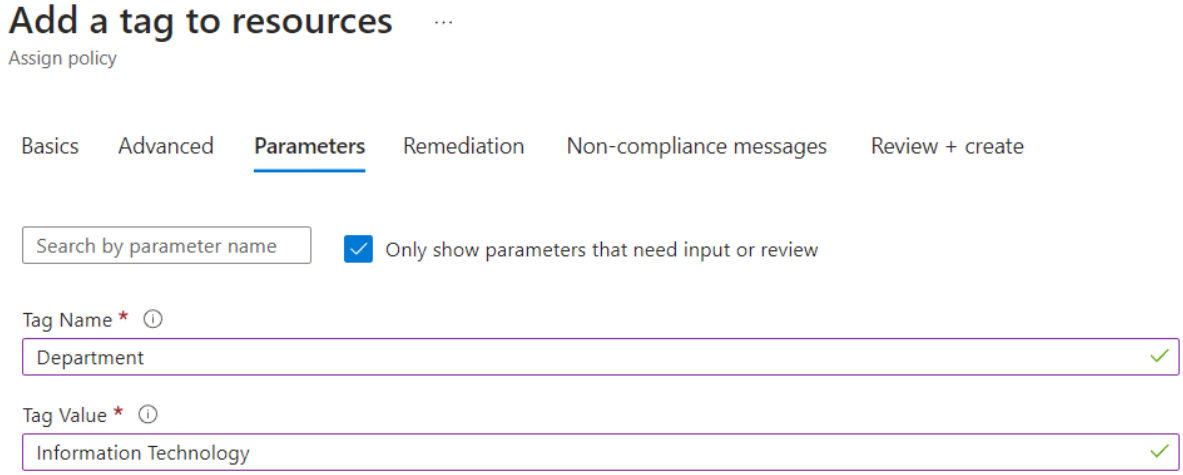
1. Now again you need to create a new Policy definition. Choose the policy shown below.



2. Click on it then on assign policy. Choose your subscription and then your resource group.



3. Now you need to go to parameters, here you need to add tag name and tag value.



4. Then you need to go to the remediation and click on create.
5. Hence, if the resources don't contain this particular tag and its value, then this remediation task is going to add the tag to the resources accordingly. Now, for this, it's going to make use of something known as a managed identity. See, because everything is based on security, Azure Policy is going to make use of the sort of identity that is going to be created in Azure Active Directory. And that identity will be given the following permissions when it comes to the contributor role. The contributor role will allow this Azure Policy Service to add a tag to its resources.

Add a tag to resources

Assign policy

Basics | Advanced | 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 a tag to 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 *

East US

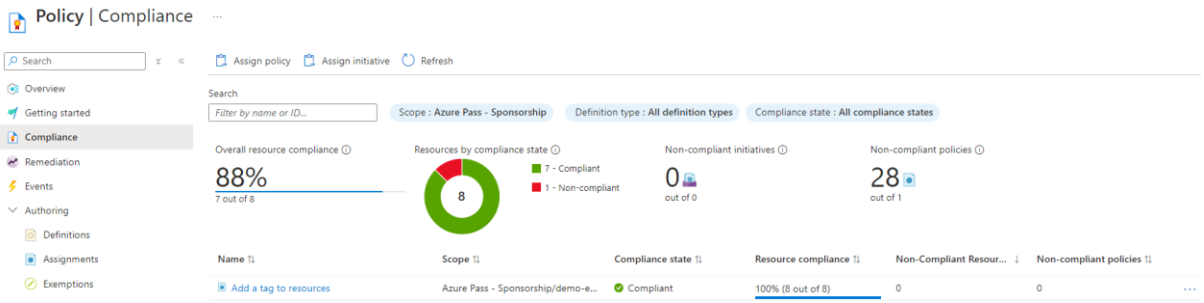
Permissions

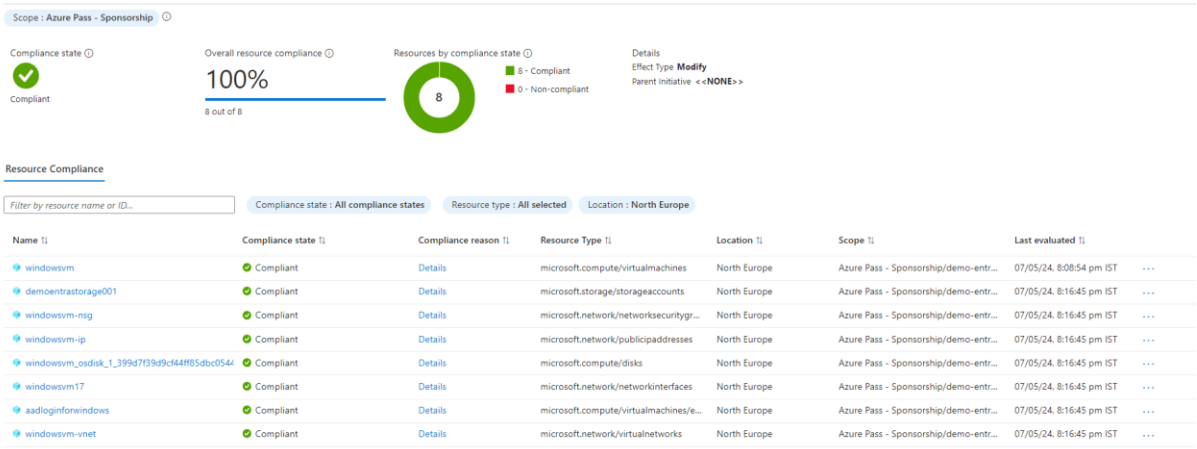
This identity will also be given the following permissions:

Contributor

ⓘ Role assignments (permissions) are created based on the role definitions specified in the policies.

6. Then just move to the review and create option and create your policy.
7. After that wait for some time. Then in the compliance tab, you can see that 100%

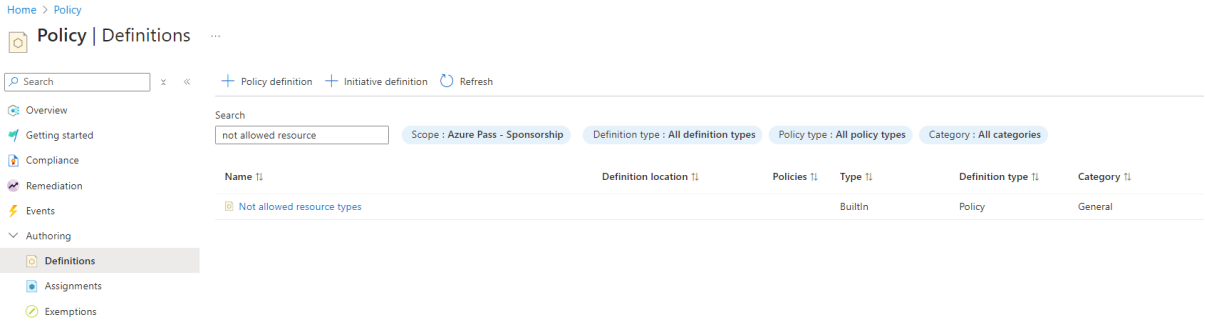




8. Now if you go inside your resources then you can see the tag there.

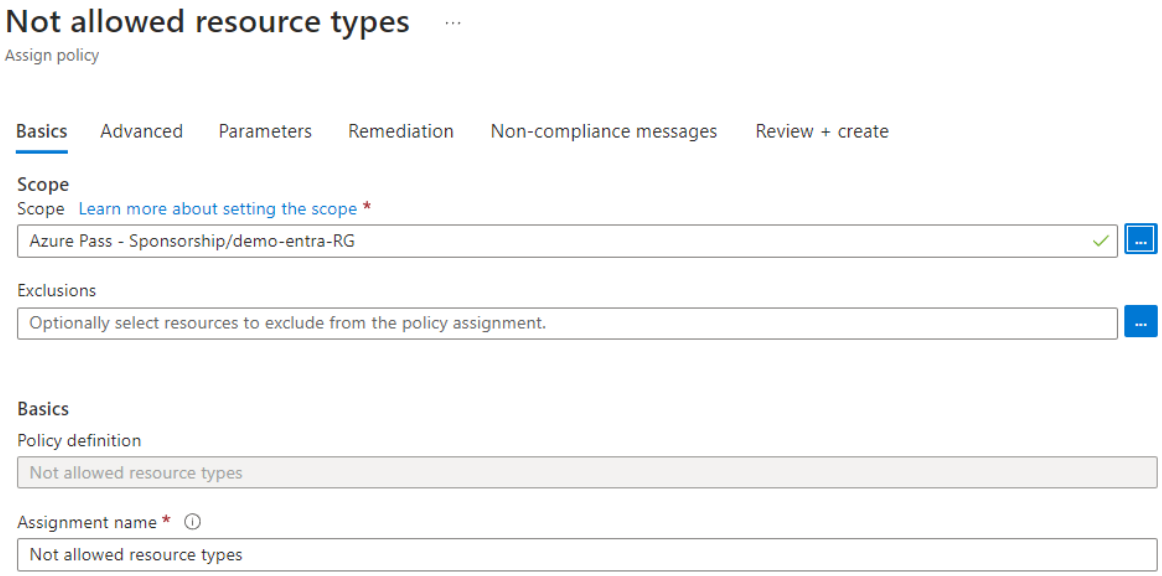
😄 Not allowed resource types

1. In your policy definitions search for the policy shown below and go inside of it.

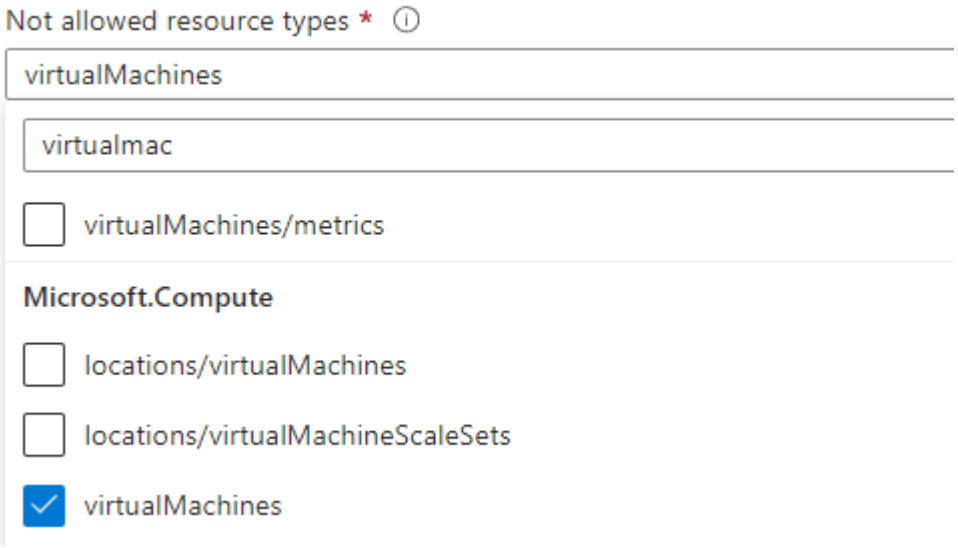


2. Then click on assign policies.

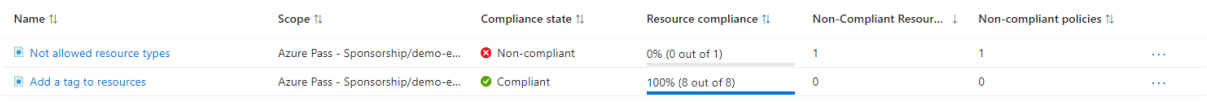
3. Choose your subscription and the resource group then move to parameters.



4. Then choose virtual machines here from Microsoft Compute.



5. Then go to the review page and create your policies.
6. Here, we've created a policy that states that the deployment of resources, as part of our selected resource group, should not contain any sort of compute-based resources that is a virtual machine.
7. Below you can see that our 2nd policy has also been created and it is non-compliant with our VM.



Name	: Not allowed resource types	Scope	: Azure Pass - Sponsorship/demo-entra-RG
Description	: --	Definition	: Not allowed resource types
Assignment ID	: /subscriptions/3541d15a-44aa-4f6e-a120-1b7a6d5925bf/resourceGroups/demo-entra-RG/prov...		

Scope : **Azure Pass - Sponsorship**

Compliance state

Non-compliant

Overall resource compliance

0%

0 out of 1

Resources by compliance state

0 - Compliant

1 - Non-compliant

Details

Effect Type **Deny**

Parent Initiative **<<NONE>>**

Resource Compliance

Filter by resource name or ID...

Compliance state : **All compliance states**

Resource type : **microsoft.compute/virtualmachines**

Location : **North Europe**

Name	Compliance state	Compliance reason	Resource Type	Location	Scope	Last evaluated
windowsvm	Non-compliant	Details	microsoft.compute/virtualmachines	North Europe	Azure Pass - Sponsorship/demo-entr...	07/05/24, 9:04:41 pm IST