😊 Azure Policy

Azure Policy is a service in Microsoft Azure that helps you manage and enforce organizational policies across your Azure resources. It allows you to create, assign, and manage policies that ensure your resources comply with organizational standards and service level agreements (SLAs). Here are some key aspects of Azure Policy:

1. **Policy Definition**: You can define policies using JSON format. These definitions specify the conditions under which the policy is enforced and the actions that are taken when the policy conditions are met.
2. **Policy Assignment**: Policies are assigned to specific scopes, which can be a subscription, resource group, or individual resources. Once assigned, the policy evaluates resources within that scope to ensure compliance.
3. **Policy Compliance**: Azure Policy continuously evaluates resources for compliance. It provides detailed compliance reports and dashboards to help you understand the compliance state of your resources.
4. **Built-in Policies**: Azure provides a wide range of built-in policy definitions for common scenarios, such as restricting certain types of resources, enforcing tagging conventions, and ensuring resource configurations meet security standards.
5. **Custom Policies**: In addition to built-in policies, you can create custom policies to address specific needs within your organization.
6. **Policy Initiatives**: A policy initiative is a collection of policies that are grouped together to achieve a specific goal. By using initiatives, you can simplify the assignment and management of multiple policies.
7. **Policy Enforcement Modes**: Policies can be enforced in different modes:
    - **Audit**: Logs non-compliant resources without preventing their creation or modification.
    - **Deny**: Prevents the creation or modification of resources that do not comply with the policy.
    - **Append**: Adds additional properties to resources during creation or update to ensure compliance.
    - **DeployIfNotExists**: Deploys a specified resource if it does not already exist to bring non-compliant resources into compliance.

Azure Policy is an essential tool for ensuring that your Azure environment remains compliant with organizational and regulatory requirements, helps in maintaining governance, and enables automation of compliance management.

😄 Use Cases of Azure Policy

Azure Policy is a versatile tool used to enforce various organizational and compliance requirements across Azure resources. Here are some common use cases:

1. **Governance and Compliance**:
    - **Enforcing Resource Tagging**: Ensure all resources are tagged with required metadata, such as cost center, environment, or owner.
    - **Compliance with Regulatory Standards**: Enforce configurations that align with standards like GDPR, HIPAA, and ISO 27001 by ensuring that necessary security controls are in place.
2. **Security**:
    - **Restricting Public Endpoints**: Prevent resources from being publicly accessible by ensuring virtual machines, storage accounts, or databases do not have public IP addresses.
    - **Enforcing Network Security Rules**: Ensure that network security groups (NSGs) have specific inbound and outbound rules for secure communication.
3. **Cost Management**:
    - **Resource Type Restrictions**: Prevent the creation of costly resource types, such as large VM sizes, to control spending.
    - **Location Restrictions**: Restrict resource deployment to specific regions to optimize costs or comply with data residency requirements.
4. **Operational Best Practices**:
    - **Ensuring Backup and Recovery**: Ensure that critical resources, like VMs and databases, have backup policies configured.
    - **Monitoring and Logging**: Enforce the enablement of monitoring and logging services, such as Azure Monitor and Azure Security Center, across all resources.
5. **Resource Configuration**:
    - **Enforcing Naming Conventions**: Ensure resources follow a specific naming convention for better organization and management.
    - **Resource SKU Enforcement**: Restrict the use of certain SKUs for resources like VMs and storage accounts to enforce standards and control costs.
6. **DevOps and Automation**:
    - **Infrastructure as Code (IaC) Compliance**: Ensure that infrastructure deployed through IaC templates (e.g., ARM templates, Terraform) complies with organizational policies.
    - **Deployment Guardrails**: Implement guardrails in CI/CD pipelines to ensure that only compliant resources are deployed.
7. **Resource Cleanup**:

- **Orphaned Resources Identification**: Identify and report resources that are not associated with any workload or application, helping to clean up unused resources.

8. **Hybrid and Multi-Cloud Management**:
    - **Consistent Policies Across Environments**: Apply the same policies across on-premises and multi-cloud environments using Azure Arc to ensure consistent governance.

🧐 What are we doing in this Lab?

In this lab, you are learning how to use Azure Policy to enforce organizational standards and ensure compliance across your Azure resources. The goal is to familiarize you with creating, assigning, and managing policies within the Azure environment. Here's a summary of the steps and the end goal:

Summary:

1. **Explore Azure Policy**: Navigate to the Azure Policy service in the Azure Portal.
2. **Understand Built-in and Custom Policies**: Learn the difference between policies and initiatives, and review built-in policy definitions.
3. **Assign a Policy**: Assign a policy (e.g., "Allowed Locations") to restrict resource creation to a specific region.
4. **Verify Compliance**: Confirm that the policy prevents the creation of resources outside the allowed region.
5. **Create and Assign Another Policy**: Assign a policy to automatically add or replace tags on resources.
6. **Test Policy Enforcement**: Create resources to see if the policies are correctly enforced (e.g., location restriction and automatic tagging).

End Goal:

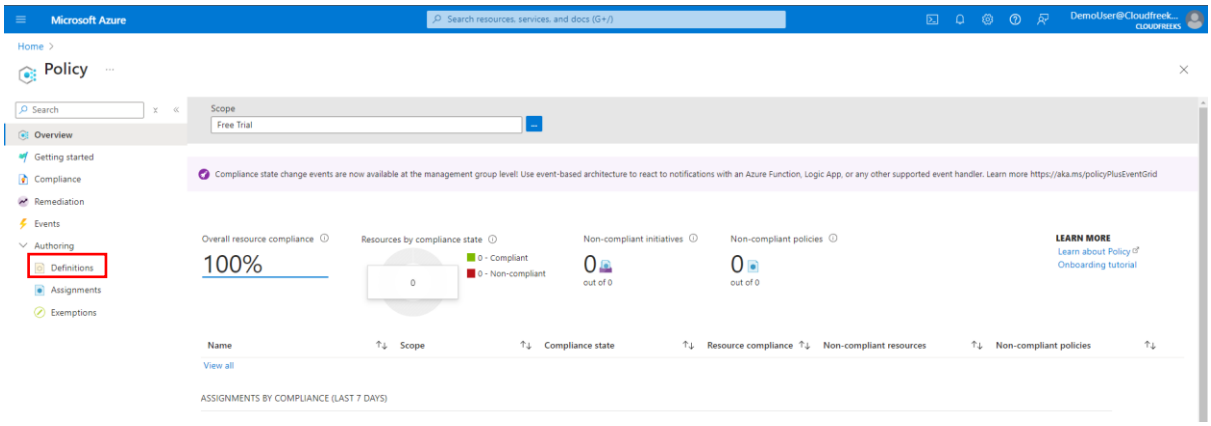
The end goal is to ensure you understand how to use Azure Policy to maintain governance, enforce compliance, and automate policy management across your Azure resources. By completing these steps, you'll be able to manage and enforce organizational standards effectively, ensuring your Azure environment remains compliant with your corporate policies and regulatory requirements.

😄 To begin with the Lab:

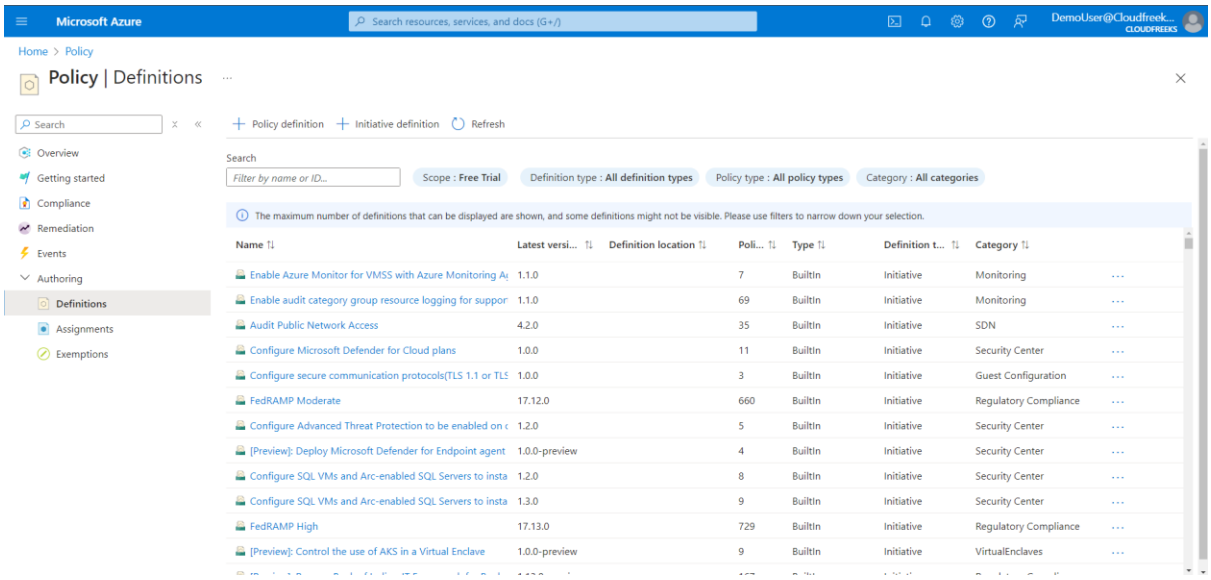
1. Azure Policy is a service in Azure that you use to create, assign, and manage policy definitions.
2. Policy definitions enforce different rules and actions over your resources, so those resources stay compliant with your corporate standards and service level agreements.
3. Azure does this by running an evaluation of your resources and scanning for those not compliant with the policy definitions you have. For example, you can have a policy to

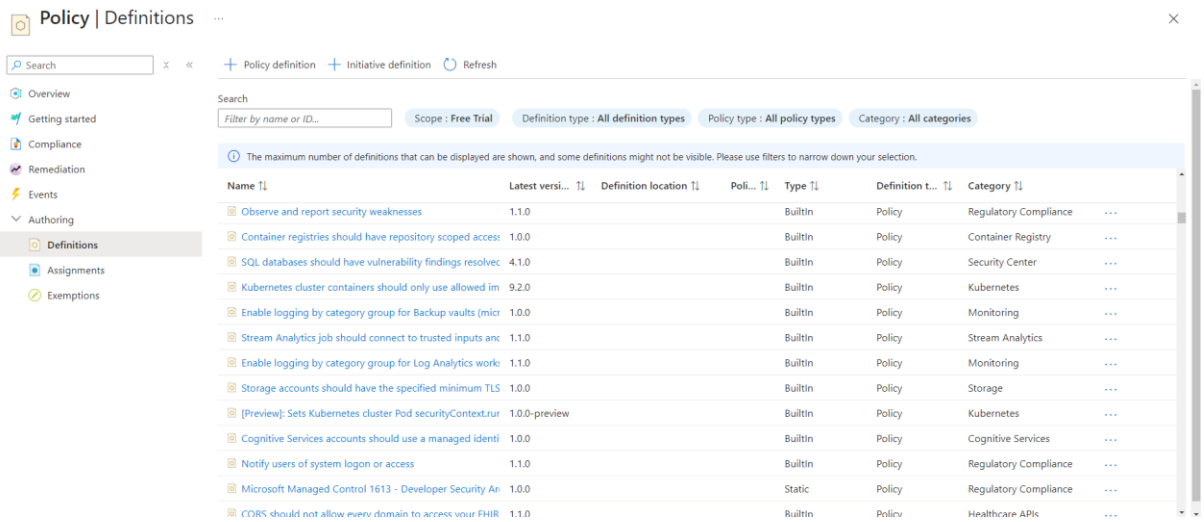
allow only certain types of virtual machines. Another requires that all resources have a particular tag. These policies are then evaluated when creating and updating resources.

4. Now in your Azure Portal you search for Azure Policy and navigate to it.
5. So, if you are visiting on Policy service for the first time then its dashboard will look like this.
6. Now if you go to definitions as it is highlighted in the snapshot.

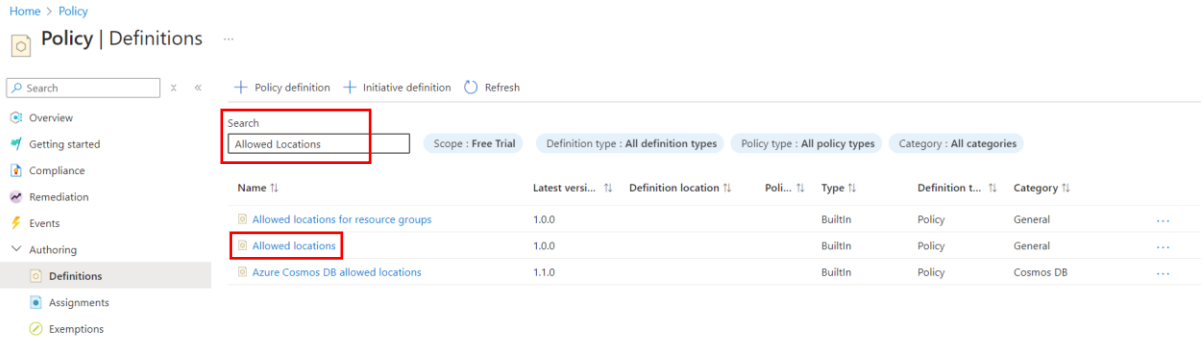


7. So, first here you will see the Builtin Initiatives, and if you scroll down then you will be able to see the Builtin Policies.
8. Also, the basic difference between policies and initiatives is that the initiatives are the collection of policy, so instead of applying a single policy you can apply a initiative which have multiple policies in it.

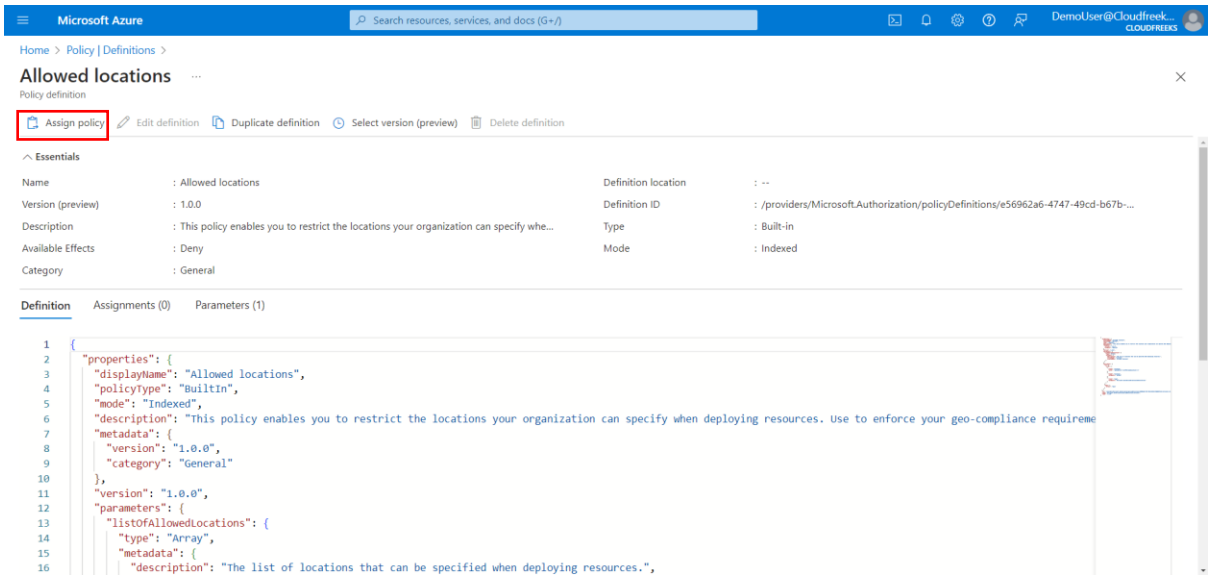




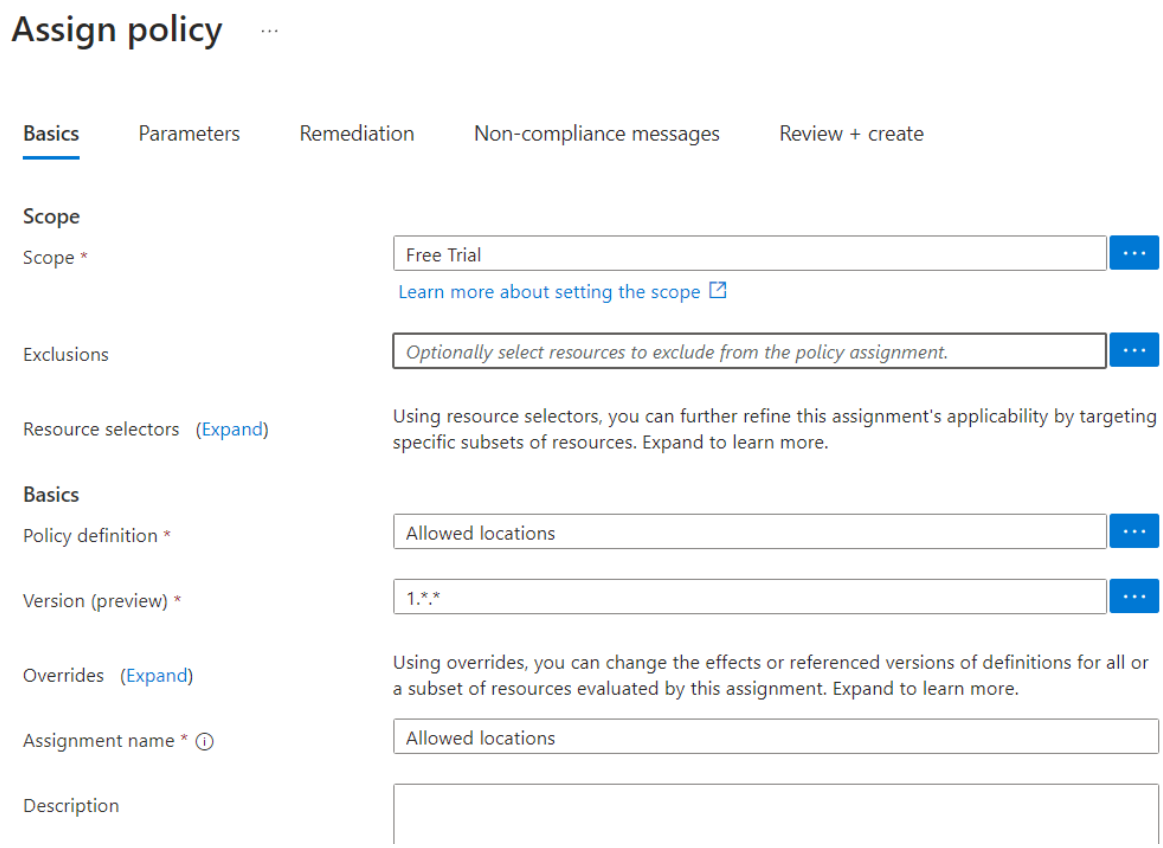
9. Now in the search option search for allowed locations, so you will see a policy which is also highlighted in the snapshot. Click on it.



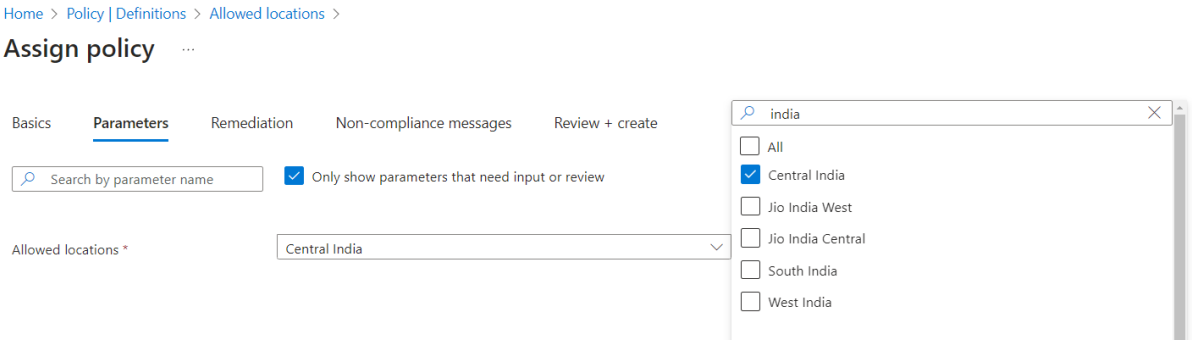
10. Then you will be inside a policy, here you can see its definition written in JSON format, and then you will see that it has been assigned to nothing as it has zero assignment. Now click on Assign Policy.



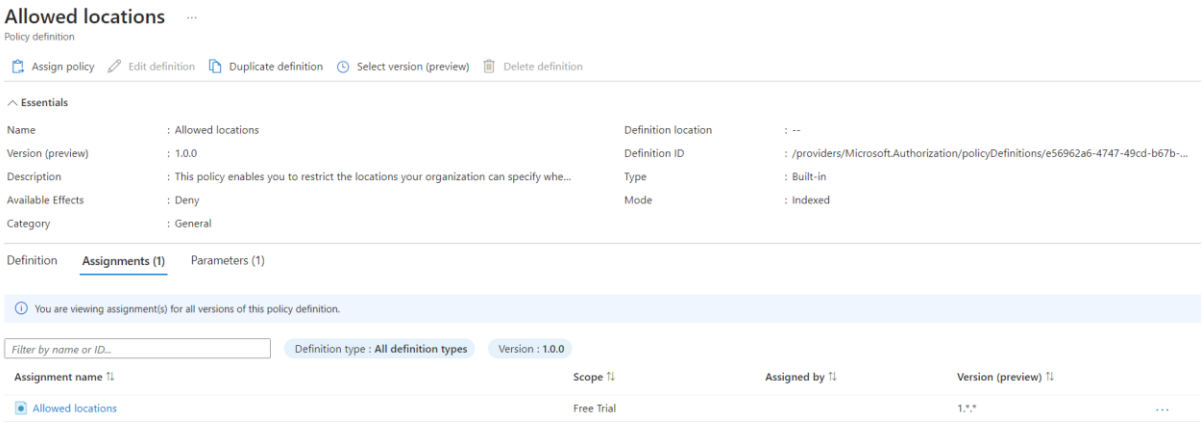
11. Now you need to choose your scope, so just choose your subscription then leave everything as it is and move to next page.



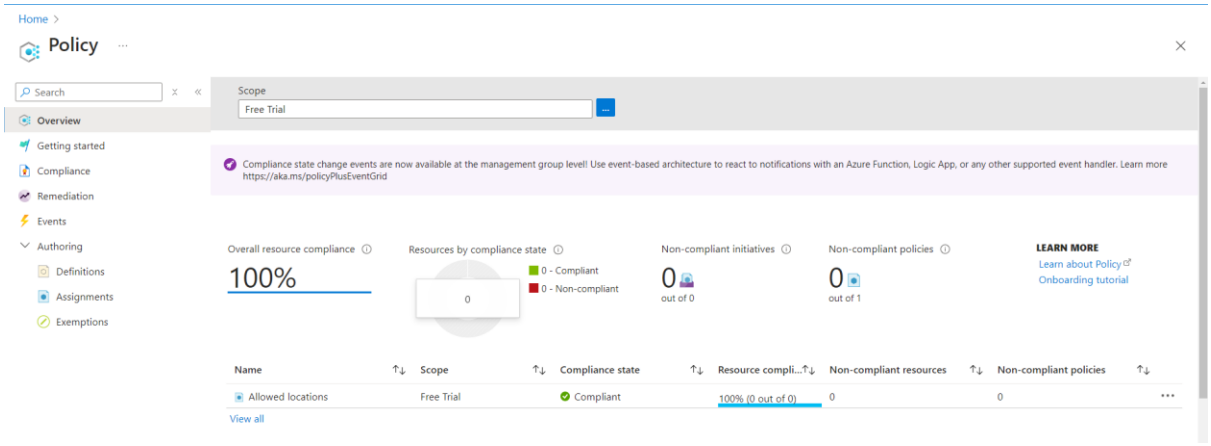
12. Then in the parameters we need to allow a location of our choice. Let's say we are allowing a location from India and it is only Central India is allowed rest are not allowed.
13. After that just move to review page and create your Policy.



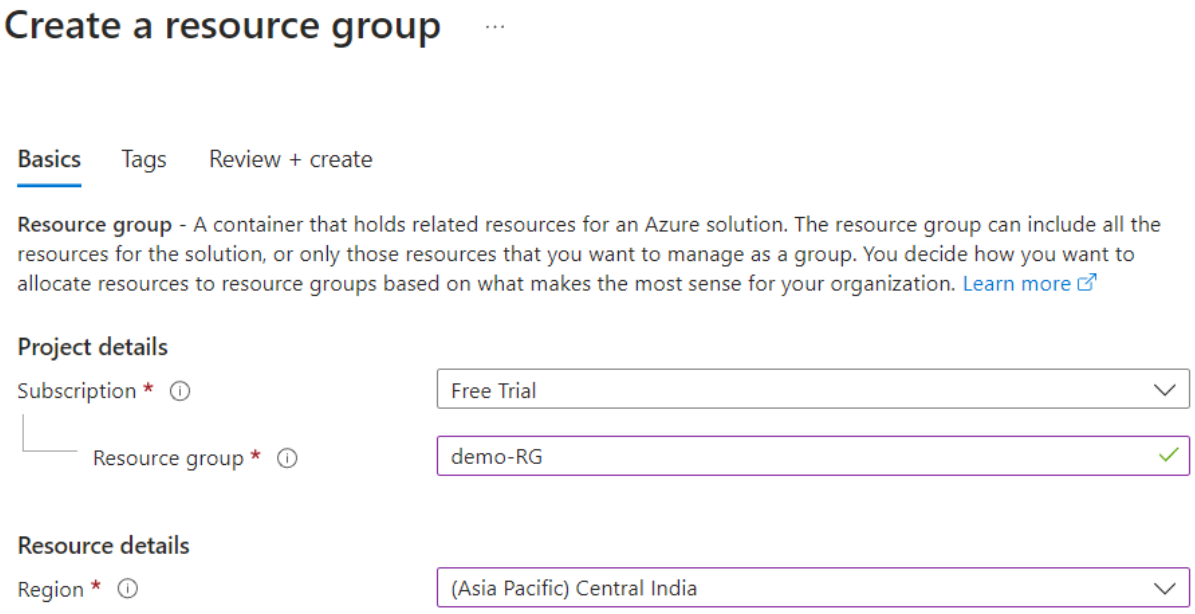
14. Once you have assigned the policy then you will see that in the assignment it is showing you to which scope it has been assigned.



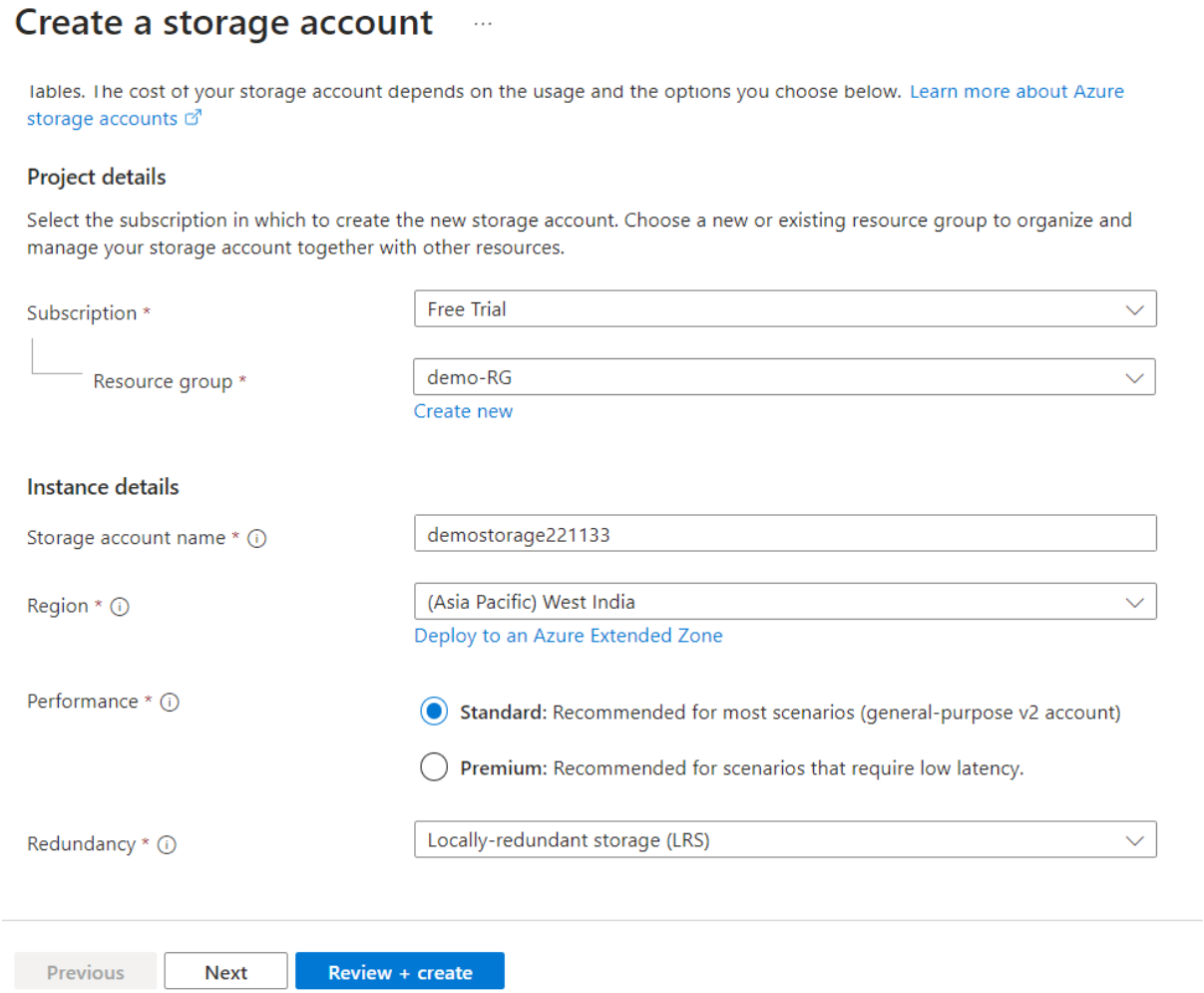
15. Then if you go to the overview of Policy, you will see that our policy is in compliant state.



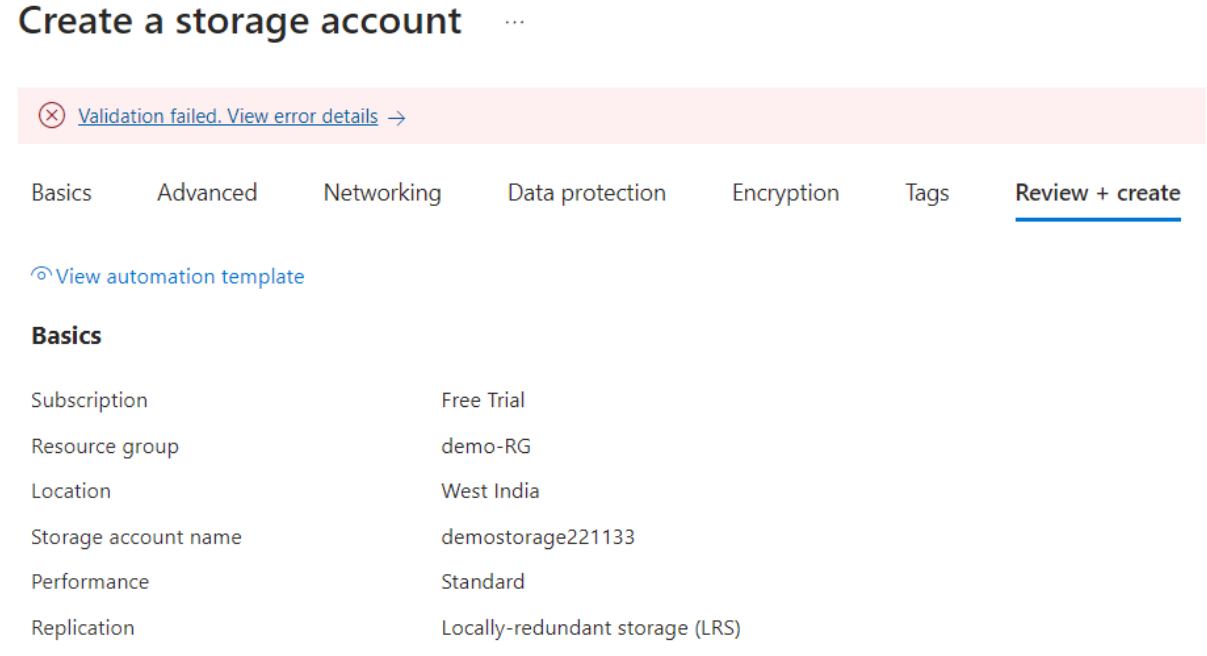
16. Now to confirm whether it is working or not. Let's go to the resource group and create one.



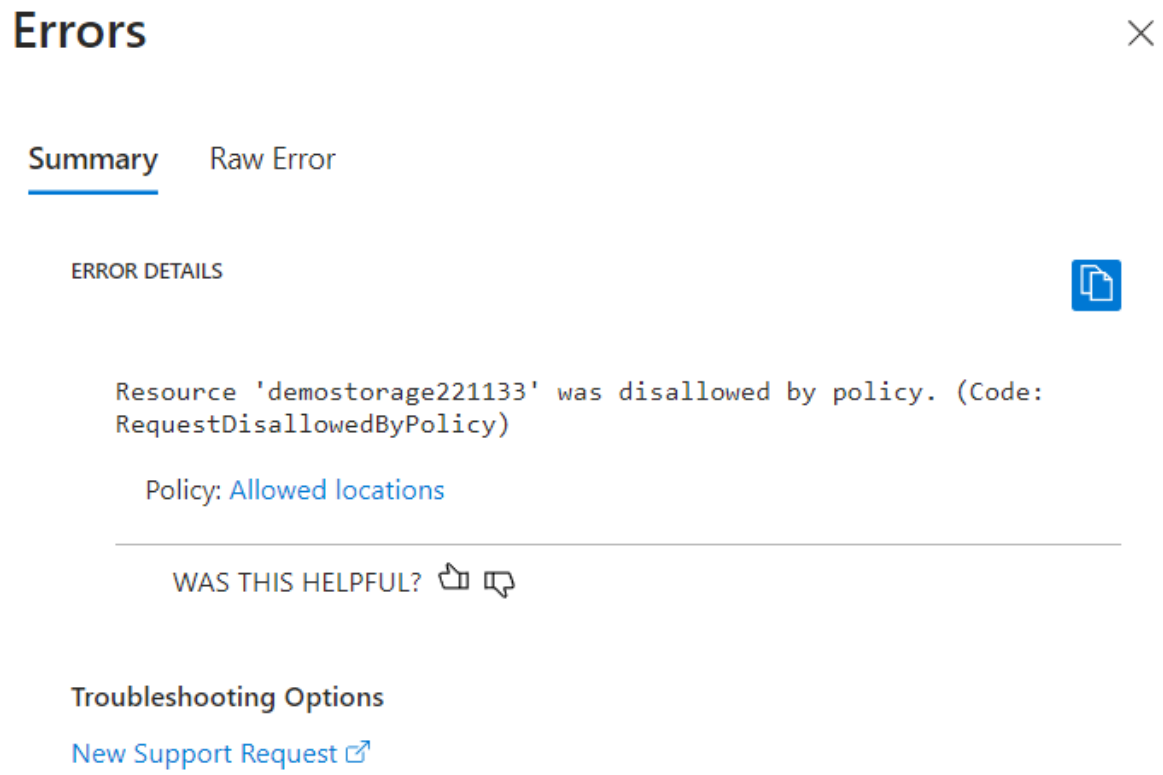
17. Once the resource group is created then we are going to create a resource in it let's say a storage account. Here we are going to choose West India as its location.



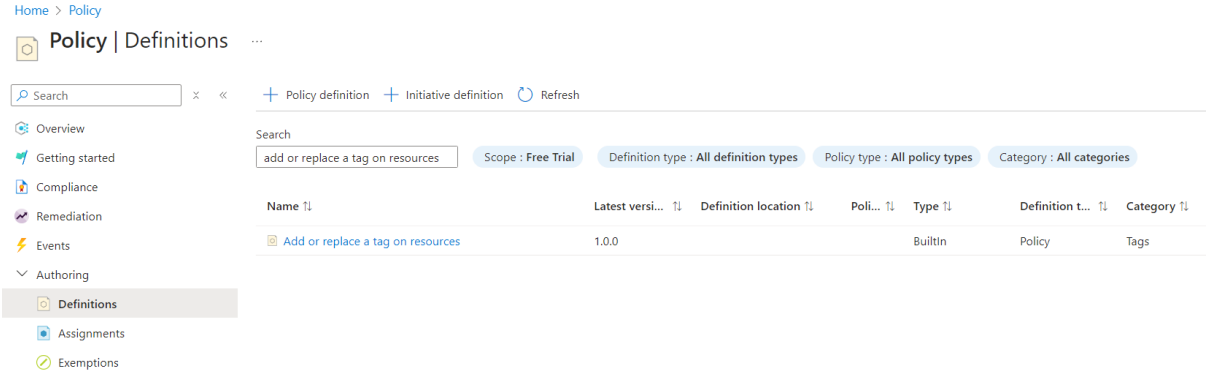
18. Below you can see that the validation has been failed.



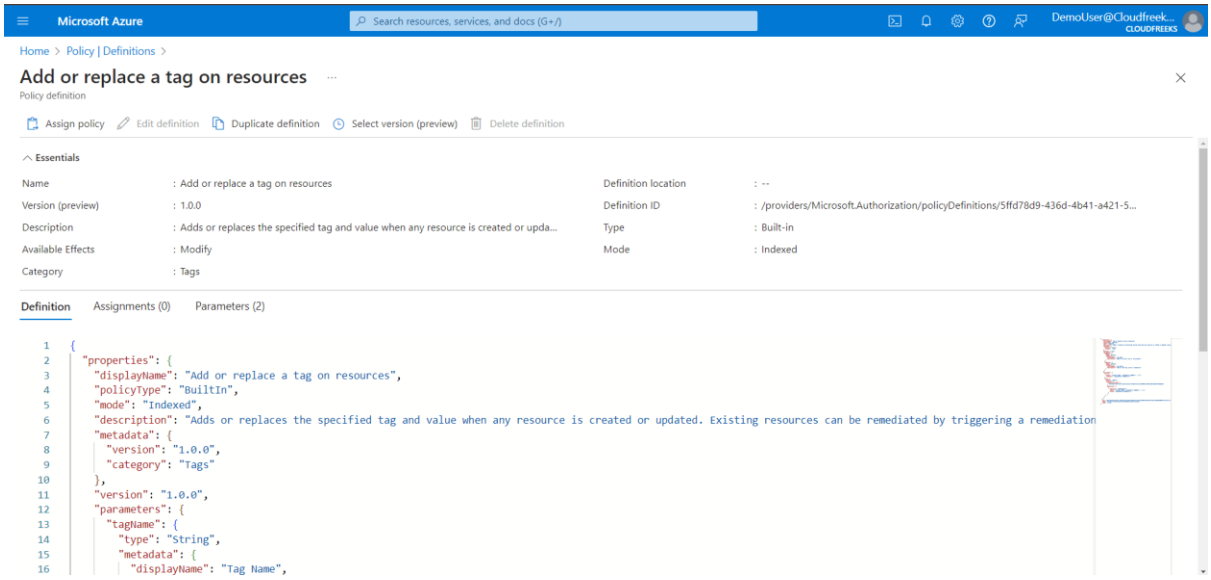
19. And if you try to see the error then you can see that it has failed because of our Allowed locations Policy.



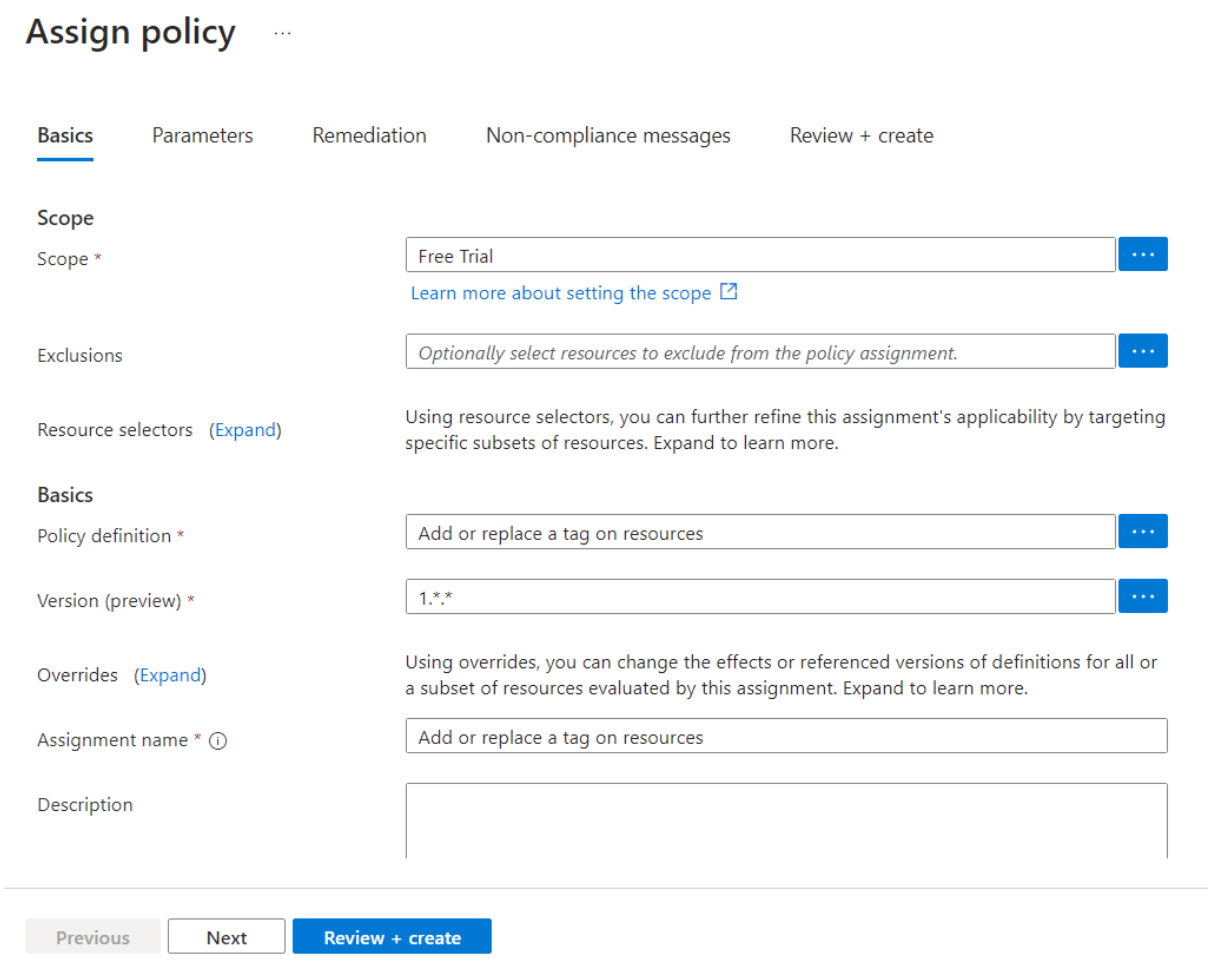
20. Now we'll try another example, again go to definitions and search for the policy mention below for add or replace a tag on resources.



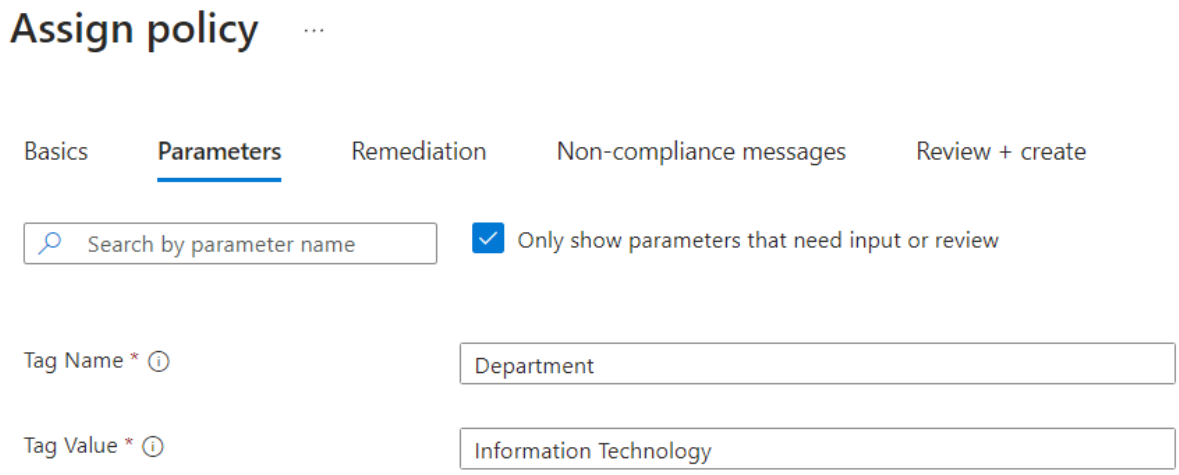
21. Again, you can see the definition of this policy, now click on assign policy.



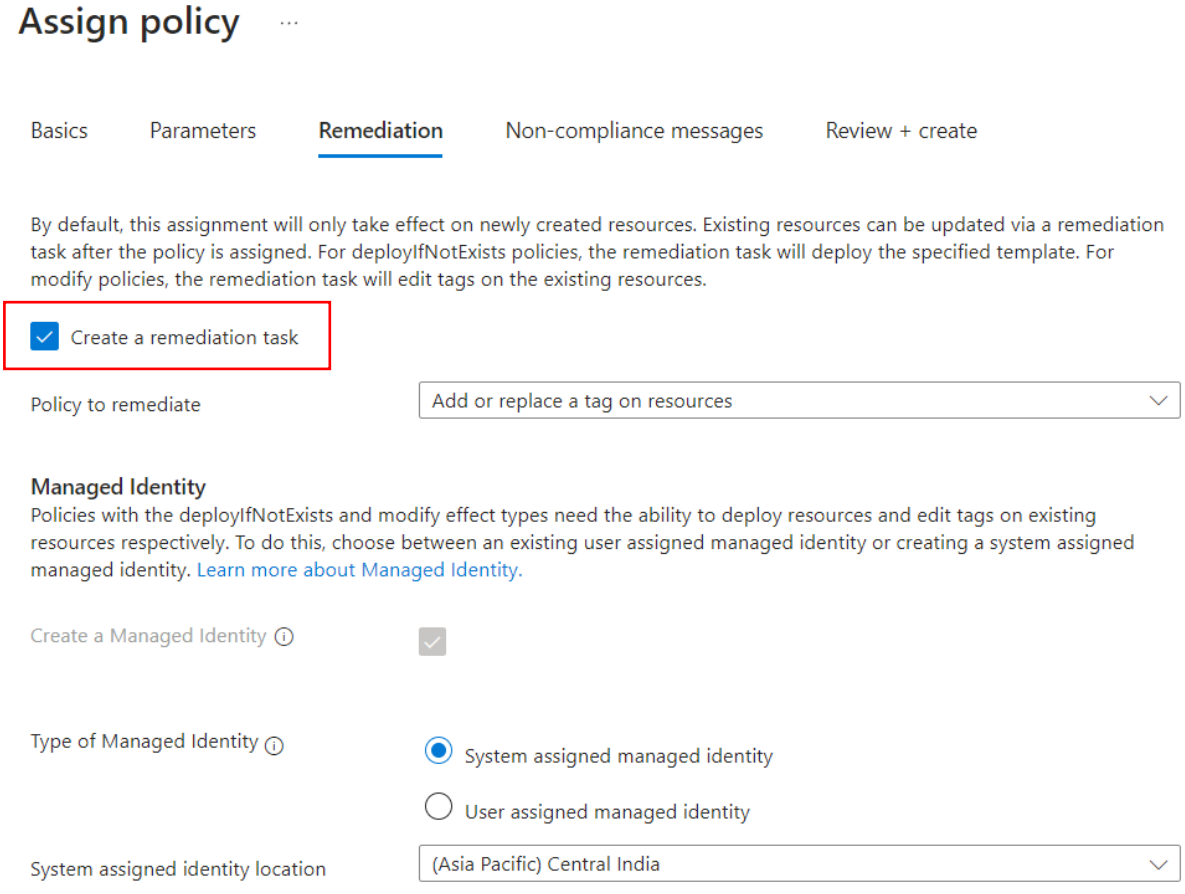
22. No change for the basic settings just leave everything as it is and move to next option.



23. Then here you need to define the tag name and value of your choice as you can see below.



24. Now in the remediation you need to allow it then move to the review page and create your policy.



25. Now we will create a resource which is a storage account. But this time we will create it in Central India as it is the only location allowed.
26. So, go to storage account and click on create. Now give it a name choose your location and move to review page then create your storage account.

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 * : Free Trial

Resource group * : demo-RG

Create new

Instance details

Storage account name * : demostorage223311

Region * : (Asia Pacific) Central India

Deploy to an Azure Extended Zone

Performance * :

- (●) **Standard:** Recommended for most scenarios (general-purpose v2 account)
- ( ) **Premium:** Recommended for scenarios that require low latency.

Redundancy * : Locally-redundant storage (LRS)

27. Once your storage account is created then go to it and navigate to tags. Below you can see that the tag has been automatically attached to our storage account.