Table of Contents

[AZURE GOVERNANCE AND COMPLIANCE 2](#_Toc159326156)

[RESOURCE TAGS 2](#_Toc159326157)

[COST MANAGEMENT ON TAGS 3](#_Toc159326158)

[MOVING RESOURCES ACROSS RESOURCE GROUPS 3](#_Toc159326159)

[MOVING RESOURCES ACROSS SUBSCRIPTIONS 3](#_Toc159326160)

[LOCKING RESOURCES 4](#_Toc159326161)

[SETTING UP RESOURCE LOCK 4](#_Toc159326162)

[LOCKS AND MOVING RESOURCES 5](#_Toc159326163)

[AZURE POLICY 5](#_Toc159326164)

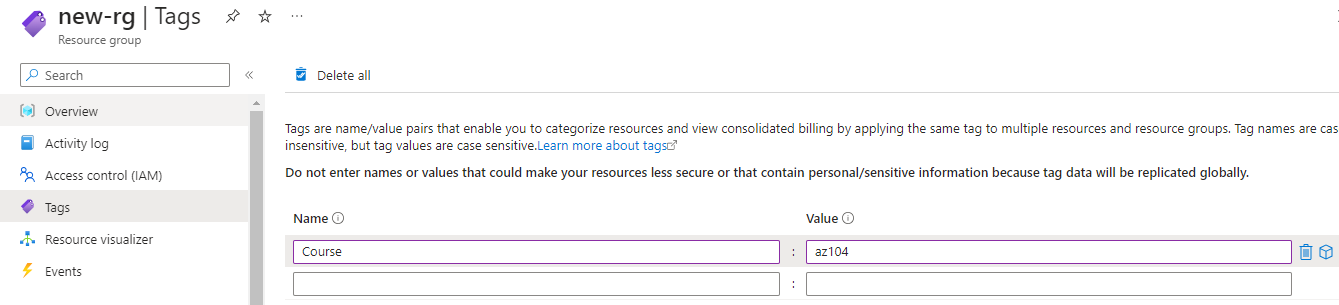
[MANAGEMENT GROUP 6](#_Toc159326165)

# AZURE GOVERNANCE AND COMPLIANCE

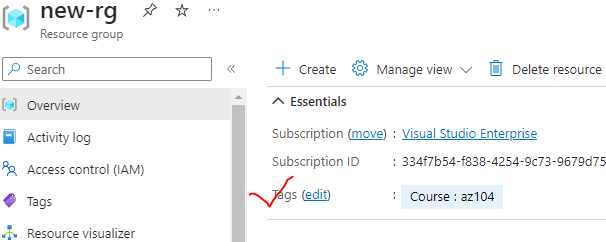
## RESOURCE TAGS

* In Azure, resource tags are metadata that we can assign to resources to organize and categorize them.
* Tags consist of name-value pairs and provide a way to add custom labels to resources.
* **We can use tags to logically group resources, track costs, apply policies, and simplify resource management**.
* Tags must be applied directly to resources and aren't implicitly inherited from the parent resource group.

**CREATING A TAG**



**TAG CREATED FOR THE RESOURCE**



**KEY POINTS ABOUT RESOURCE TAGS**

* TAG STRUCTURE:
  + Tags consist of a name and a value. The name is a string, and the value can be any string or empty.
* TAG LIMITATIONS:
  + Each resource can have multiple tags, up to a **maximum of 50 tags per resource.**
  + Tag names are case-insensitive, and the tag name-value pairs must be unique within a resource.
* ASSIGNING TAGS:
  + Tags can be assigned to resources during creation or added later.
  + We can assign tags using Azure Portal, Azure PowerShell, Azure CLI, or Azure Resource Manager templates.
* MANAGING TAGS:
  + We can manage and view tags for resources through the Azure Portal, Azure PowerShell, Azure CLI, Azure Resource Manager templates, or Azure Management APIs.
  + Tags can also be used for filtering, organizing, and querying resources.
* COST MANAGEMENT:
  + By assigning tags to resources, we can track and manage costs associated with those resources.
  + Azure Cost Management + Billing provides reporting and analysis capabilities based on resource tags.
* POLICY ENFORCEMENT:
  + Azure Policy allows us to define policies based on tags to enforce compliance and governance rules.
  + We can use policies to ensure resources have specific tags assigned or to restrict resource creation based on tags.

## COST MANAGEMENT ON TAGS

## MOVING RESOURCES ACROSS RESOURCE GROUPS

* In Azure, we can move resources across resource groups using the **Azure Portal, Azure PowerShell, Azure CLI, or Azure Resource Manager templates**. Here's how you can perform this task using each method:

Azure Portal:

1. Open the Azure Portal and navigate to the resource you want to move.
2. Select "Move" from the resource's menu.
3. Choose the "Move to another resource group" option.
4. Select the target resource group and click "OK" to initiate the move.

Azure PowerShell:

1. Open Azure PowerShell and connect to your Azure account.
2. Use the Get-AzResource cmdlet to retrieve the resource you want to move.
3. Use the Move-AzResource cmdlet to move the resource to the target resource group.  
   Example: Move-AzResource -ResourceId <resourceId> -DestinationResourceGroupName <targetResourceGroup>

Azure CLI:

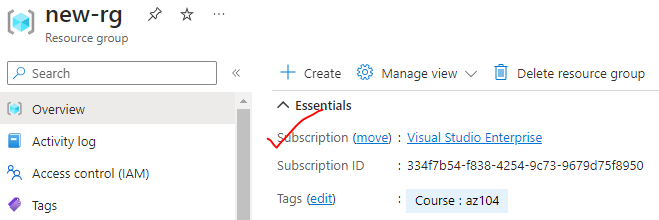
1. Open Azure CLI and sign in to your Azure account.
2. Use the az resource show command to get the details of the resource you want to move.
3. Use the az resource move command to move the resource to the target resource group.  
   Example: az resource move --ids <resourceId> --destination-group <targetResourceGroup>

## MOVING RESOURCES ACROSS SUBSCRIPTIONS

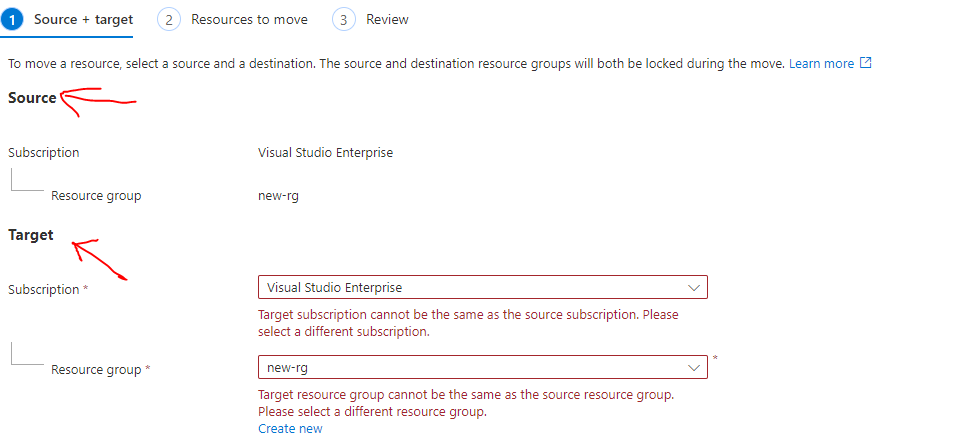
* We can move resources across subscriptions using the Azure Portal or Azure PowerShell.

USING AZURE PORTAL

* Open the Azure Portal and navigate to the resource you want to move.
* Select "Move" from the resource's menu.



* Choose the "Move to another subscription" option.
* Select the target subscription and click "OK" to initiate the move.



AZURE POWERSHELL

1. Open Azure PowerShell and connect to your Azure account.
2. Use the Get-AzResource cmdlet to retrieve the resource you want to move.
3. Use the Move-AzResource cmdlet to move the resource to the target subscription.  
   Example: Move-AzResource -ResourceId <resourceId> -DestinationSubscriptionId <targetSubscriptionId>

WHEN MOVING RESOURCES ACROSS SUBSCRIPTIONS, THERE ARE A FEW IMPORTANT CONSIDERATIONS:

* Permissions:
  + We need appropriate permissions in both the source and target subscriptions to perform the move operation.
* Limitations:
  + Not all resources can be moved across subscriptions.
  + Some resources, **like virtual networks and storage accounts**, have limitations or dependencies that may prevent the move.
* Resource Dependencies:
  + When moving resources with dependencies, we may need to move related resources as well.
  + **For example, if you're moving a virtual machine, we might need to move its associated network interface and storage account.**
* Resource Group: Moving a resource to another subscription may require moving its associated resource group as well. Make sure to consider the impact on other resources in the same resource group.

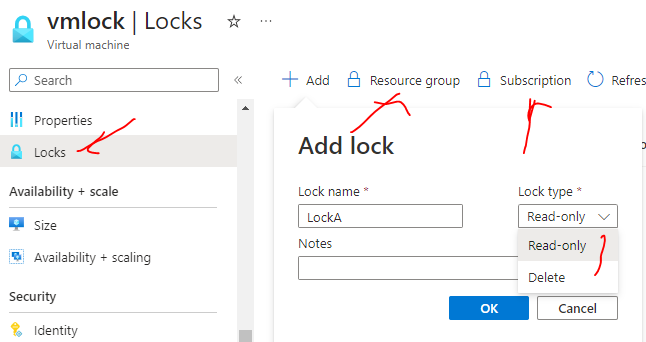
## LOCKING RESOURCES

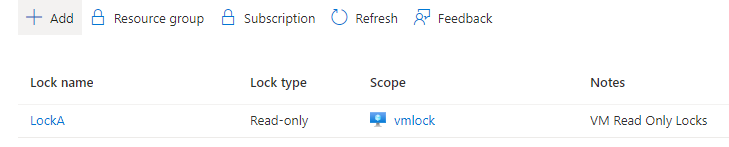
* In Azure, resource locks are a feature that allows us to **prevent accidental deletion or modification of critical resources.**
* By applying a lock to a resource or resource group, we can ensure that it cannot be deleted or modified without explicit permission. This helps in maintaining the integrity and stability of important resources.

HERE ARE A FEW KEY POINTS ABOUT RESOURCE LOCKS IN AZURE:

* TYPES OF LOCKS: There are two types of locks you can apply to resources:
  + Delete Lock (CanNotDelete): This lock prevents the resource from being deleted, but it allows other modifications.
  + Read-Only Lock(ReadOnly): This lock makes the resource read-only, preventing both deletion and modifications.
* SCOPE:
  + We can apply locks at the resource group level or at the individual resource level.
  + **Applying a lock at the resource group level automatically applies it to all resources within that group**.
* LOCK HIERARCHY:
  + Locks have a hierarchical relationship, meaning a lock applied at a parent level (resource group) is inherited by child resources unless overridden.
  + For example – the Locks on resource group level will apply the lock to all the resources in the resource group. Similarly the locks on subscription level will apply the lock to all the resources in that subscription

### SETTING UP RESOURCE LOCK





* **As “ReadOnly“ locks has been applied to the VM – we cannot perform any operation or modify any of the property of the VM.**

### LOCKS AND MOVING RESOURCES

* **If the resource has lock we still have the ability to move the resource across the resource groups.**
* **If applied a lock at the resource group level, then the lock will be inherited to the resources in the resource group. If we try to move the resource to different resource group – then we cannot move the resource because we are changing the properties of the resource group.**
* if we lock the destination resource group even then we can't move the resources to the destination resource group

## AZURE POLICY

* Azure Policy Service is a governance service in Microsoft Azure that allows us to enforce and monitor compliance with organizational standards and best practices across your Azure environment.
* It provides a centralized way to define, assign, and enforce policies that govern resource configurations and behaviors.  
    
  Here are some key features and capabilities of Azure Policy Service:
* Policy definition: Azure Policy allows you to define policies using JSON-based rules that specify the desired state and behavior of Azure resources. Policies can cover a wide range of aspects, such as resource properties, tagging, access control, network security, and more.
* Policy assignment: Once policies are defined, you can assign them to Azure subscriptions, resource groups, or management groups. This allows you to apply policies at different scopes, depending on your governance requirements.
* Compliance evaluation: Azure Policy continuously evaluates resources against assigned policies and provides compliance results. It helps identify resources that are non-compliant, allowing you to take corrective actions to bring them into compliance.
* Policy enforcement: Azure Policy can enforce compliance by blocking the creation or modification of resources that violate policy rules. It can also trigger notifications or remediation actions to rectify non-compliant resources.
* Built-in and custom policies: Azure Policy offers a range of built-in policies that cover common governance scenarios. Additionally, you can create custom policies tailored to your specific requirements using Azure Policy's JSON-based policy definition language.
* Integration with Azure DevOps and CI/CD pipelines: Azure Policy integrates with Azure DevOps and CI/CD pipelines, enabling you to include policy validation as part of your deployment and release processes.  
    
  Azure Policy Service helps you maintain control and enforce governance across your Azure environment by providing a mechanism to define, assign, and enforce policies. It promotes best practices, improves security, and ensures compliance with organizational standards and regulatory requirements.

## MANAGEMENT GROUP

* In Azure, Management Groups are a hierarchical organizational construct that allow us to manage and govern resources across multiple Azure subscriptions.
* Management Groups provide a way to apply policies, access control, and governance at scale by creating a hierarchy of groups.