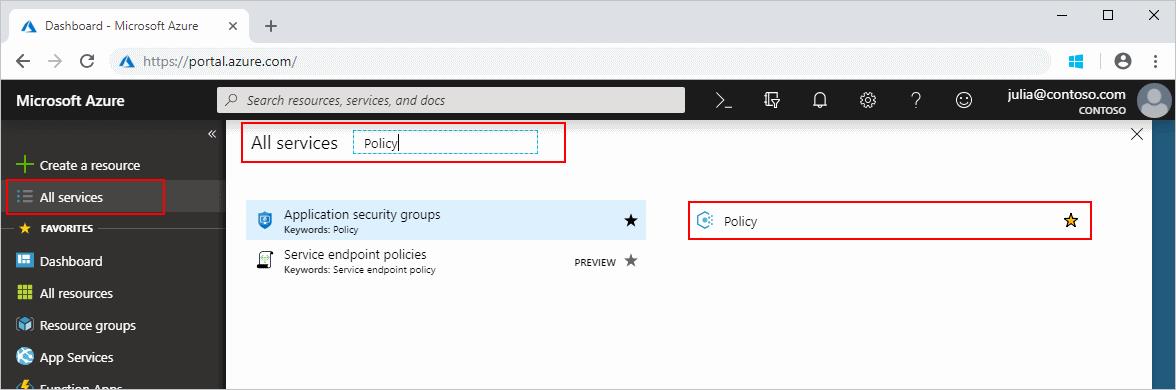
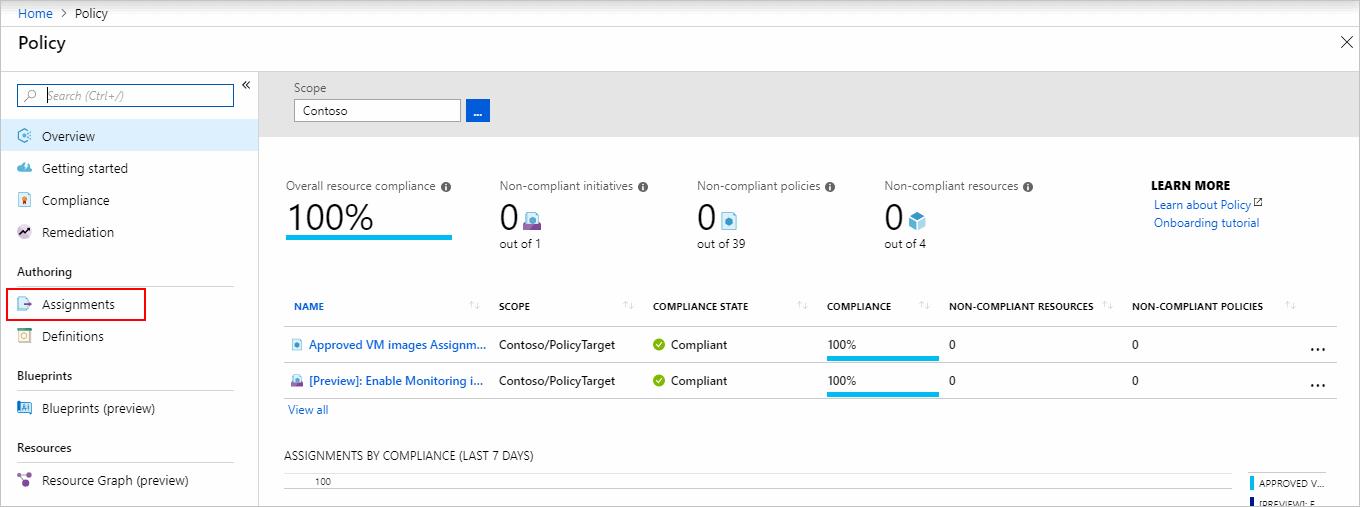
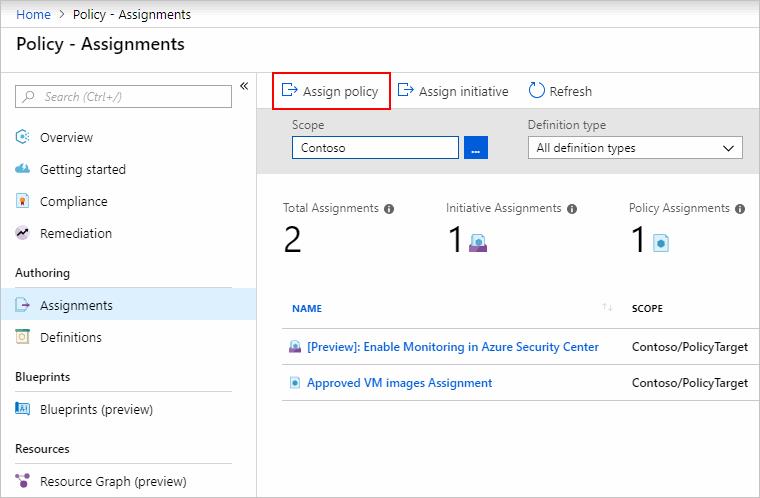
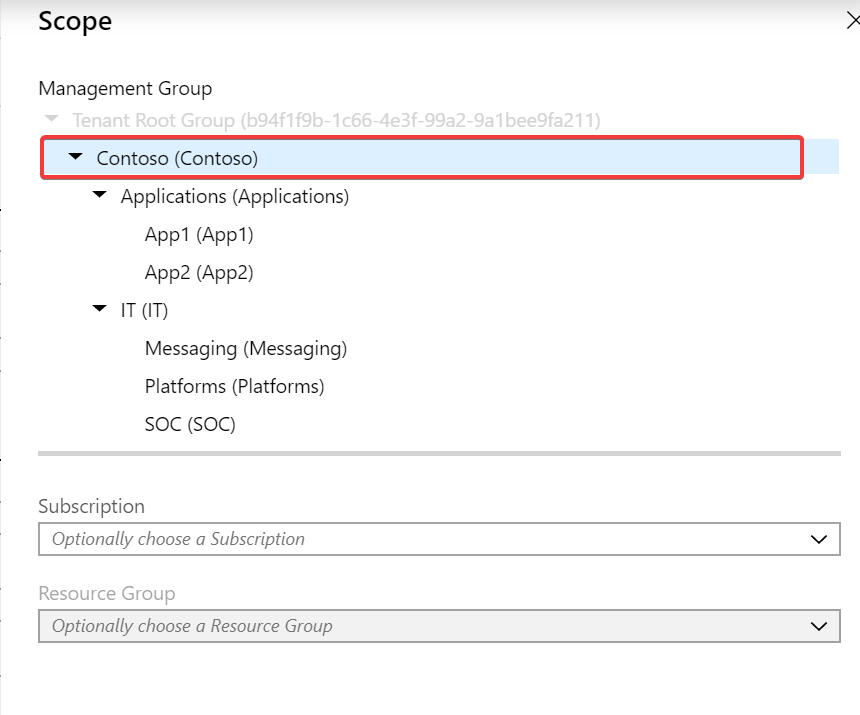
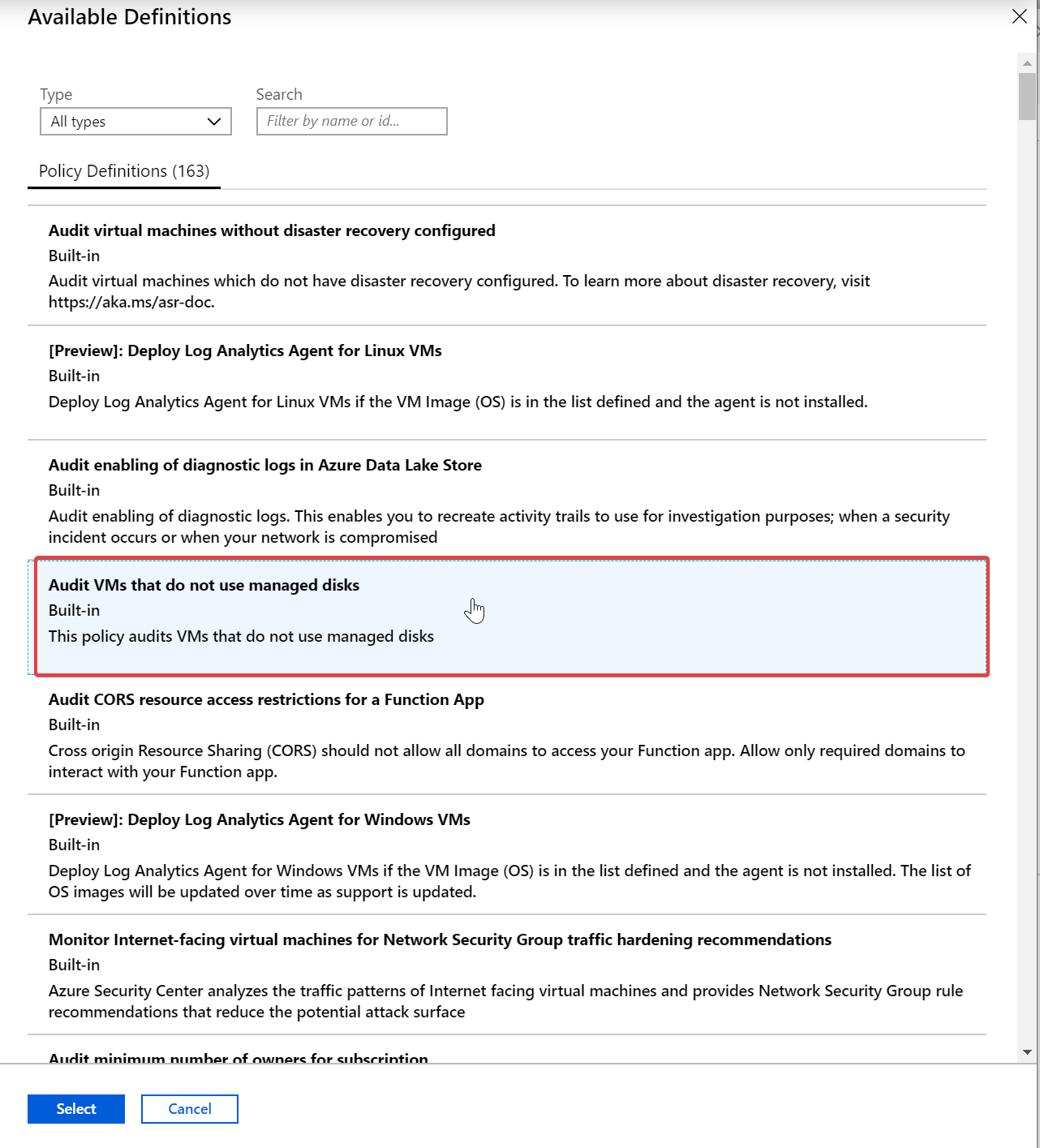
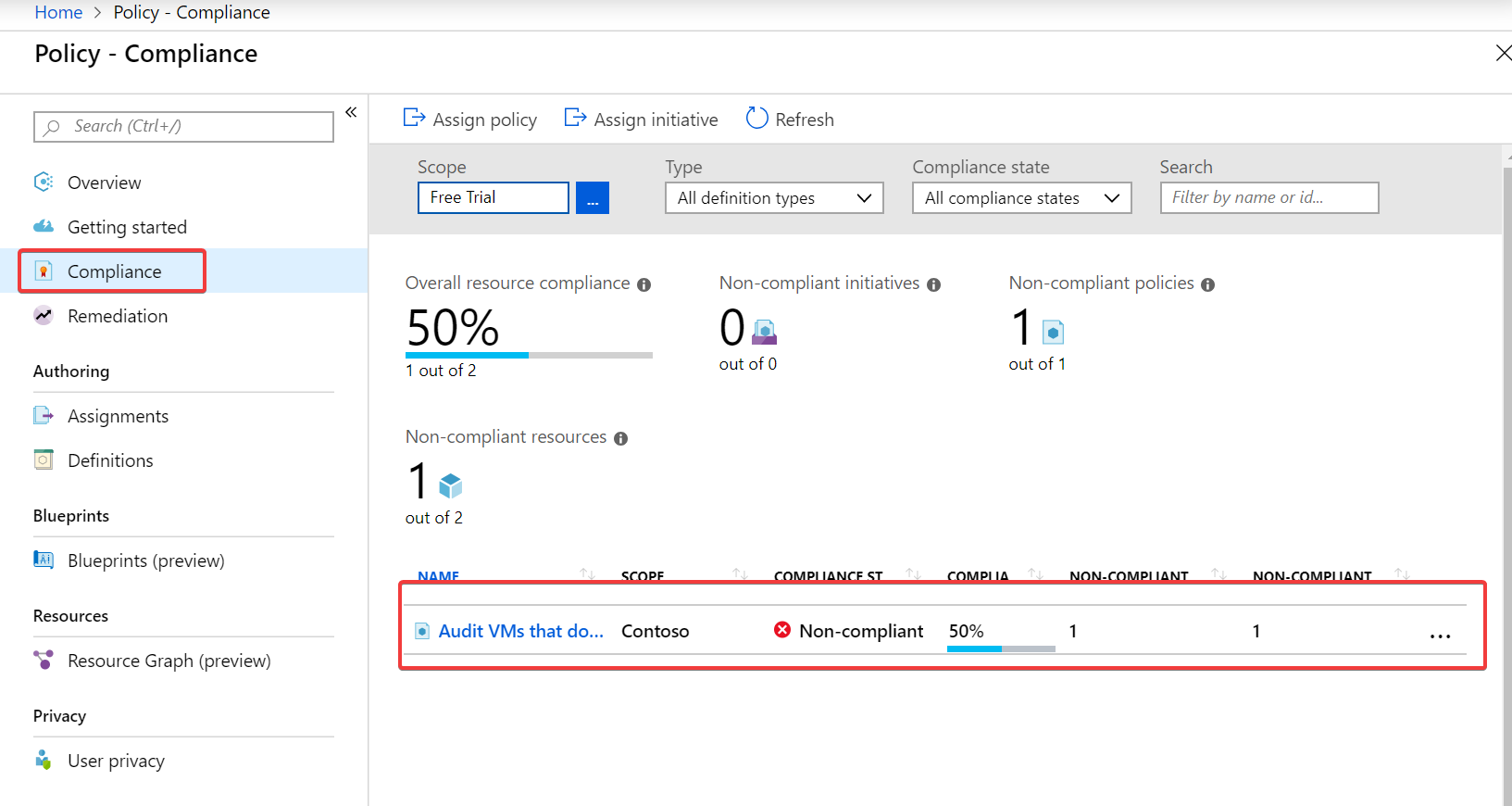
Challenge 2: Create a policy assignment to identify non-compliant resources in your Azure environment

Scenario

The first step in understanding compliance in Azure is to identify the status of your resources. This exercise steps you through the process of creating a policy assignment to identify virtual machines that aren't using managed disks. At the end of this process, you'll successfully identify virtual machines that aren't using managed disks. They're non-compliant with the policy assignment.

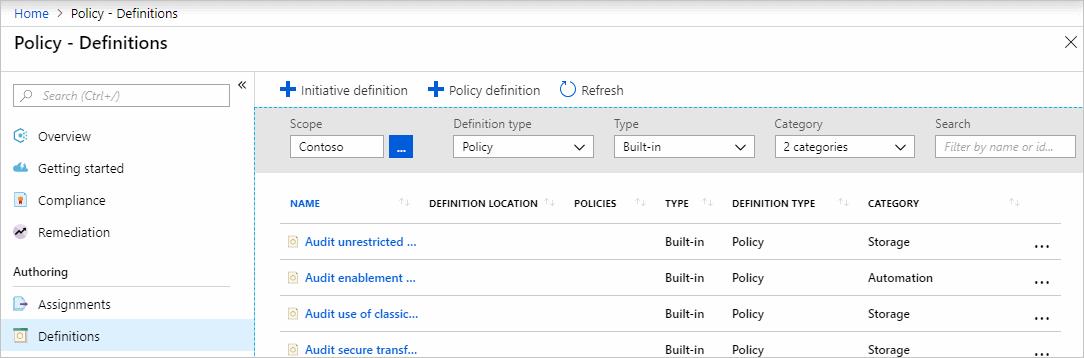
**Note**: Make sure you have deployed the VMs outlined in the Azure Governance Workshop Setup Guide.

Create a policy assignment

* 1. Launch the Azure Policy service in the Azure portal by clicking **All services**, then searching for and selecting Policy.  
     
  2. Select Assignments on the left side of the Azure Policy page. An assignment is a policy that has been assigned to take place within a specific scope.  
     
  3. Select **Assign Policy** from the top of the **Policy - Assignments** page.  
     
  4. On the **Assign Policy** page, select the Scope by clicking the ellipsis and select the Contoso Management Group.  
        
     Then click **Select** at the bottom of the Scope page.
  5. Resources can be excluded based on the Scope. Exclusions start at one level lower than the level of the Scope. Exclusions are optional, so leave it blank for now.
  6. Select the Policy definition ellipsis to open the list of available definitions. Azure Policy comes with built-in policy definitions you can use. Many are available, such as:
  + Enforce tag and its value
  + Apply tag and its value
  + Require SQL Server version 12.0
  + Search through the policy definitions list to find the Audit VMs that do not use managed disks definition.   
      
    Click on that policy and click Select.
  1. The **Assignment name** is automatically populated with the policy name you selected, but you can change it. For this example, leave *Audit VMs that do not use managed disks*. You can also add an optional **Description**. The description provides details about this policy assignment. **Assigned by**will automatically fill based on who is logged in. This field is optional, so custom values can be entered.
  2. Leave **Create a Managed Identity** unchecked. This box must be checked when the policy or initiative includes a policy with the *[deployIfNotExists](https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects" \l "deployifnotexists)* effect. As the policy used for this quickstart doesn't, leave it blank.
  3. Click **Assign**.  
     You’re now ready to identify non-compliant resources to understand the compliance state of your environment.  
     

Implement a new custom policy

Now that you've assigned a built-in policy definition, you can do more with Azure Policy. Next, create a new custom policy to save costs by validating that VMs created in your environment can't be in the G series. This way, every time a user in your organization tries to create VM in the G series, the request is denied.

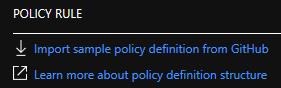
* 1. Select **Definitions** under **Authoring** in the left side of the Azure Policy page.  
     
  2. Select **+ Policy definition** at the top of the page. This button opens to the Policy definition page.
  3. Enter the following information:
  + The Applications Management Group in which the policy definition is saved. Select by using the ellipsis on Definition location.

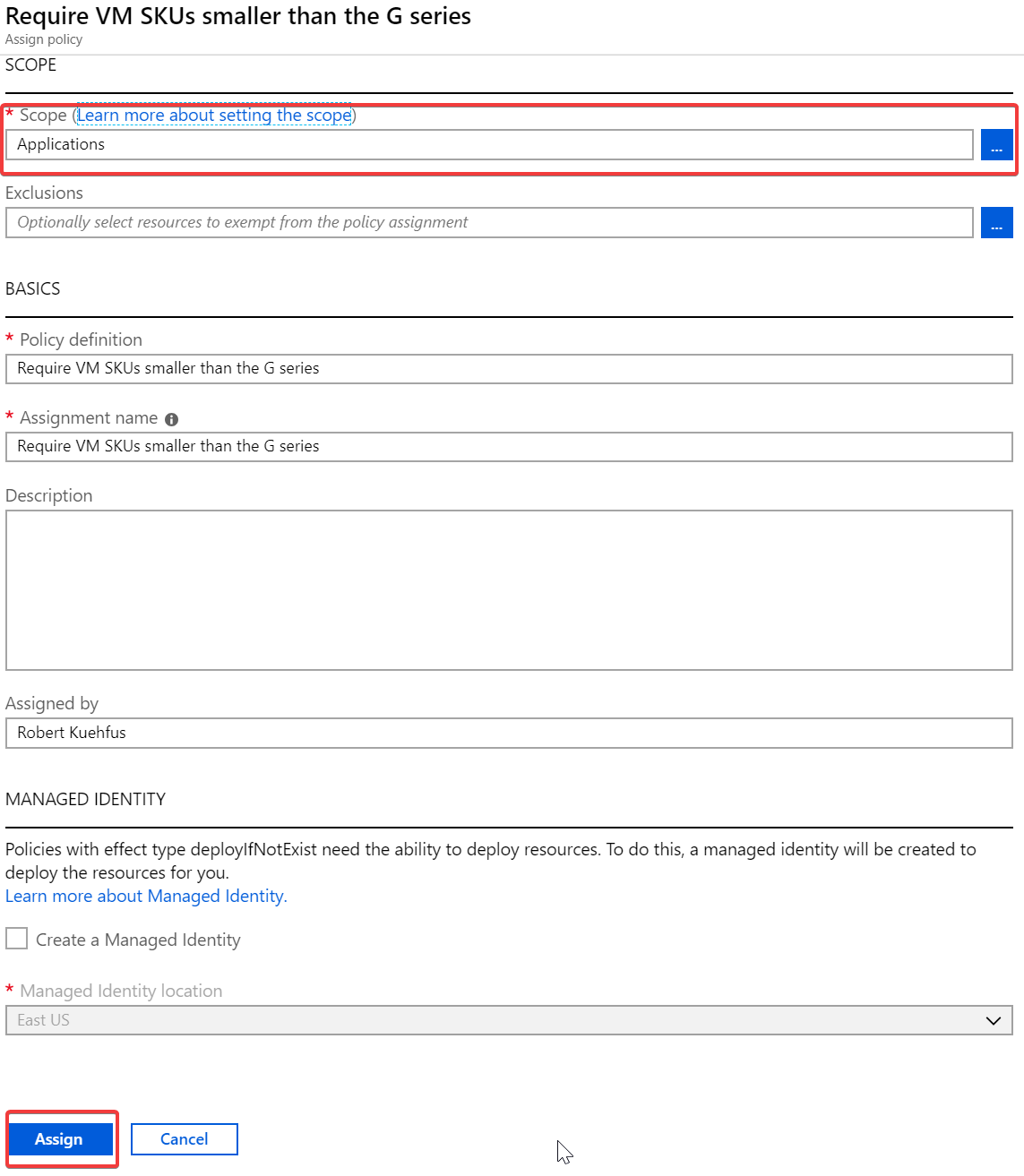
If you plan to apply this policy definition to multiple subscriptions, the location must be a management group that contains the subscriptions you assign the policy to. The same is true for an initiative definition.

* + The name of the policy definition - Require VM SKUs smaller than the G series
  + The description of what the policy definition is intended to do – This policy definition enforces that all VMs created in this scope have SKUs smaller than the G series to reduce cost.
  + Choose from existing options (such as Compute), or create a new category for this policy definition.
  + Copy the following JSON code and then update it for your needs with:
    1. The policy parameters.
    2. The policy rules/conditions, in this case – VM SKU size equal to G series
    3. The policy effect, in this case – Deny.

{  
 "policyRule": {  
 "if": {  
 "allOf": [{  
 "field": "type",  
 "equals": "Microsoft.Compute/virtualMachines"  
 },  
 {  
 "field": "Microsoft.Compute/virtualMachines/sku.name",  
 "like": "Standard\_G\*"  
 }  
 ]  
 },  
 "then": {  
 "effect": "deny"  
 }  
 }  
}

Not that you can import sample policy definition from GitHub



* + Select Save.
  1. Now assign the newly created policy to the Applications Management Group.  
       
     Click Assign
  2. Once Assigned attempt to deploy a G series VM in East US 2 from the Cloud Shell.

#Create Resource Group for managed disk VM

ResourceGroupName="Contoso\_GSeries"

az group create --name $ResourceGroupName --location eastus2

az vm create \

--resource-group $ResourceGroupName \

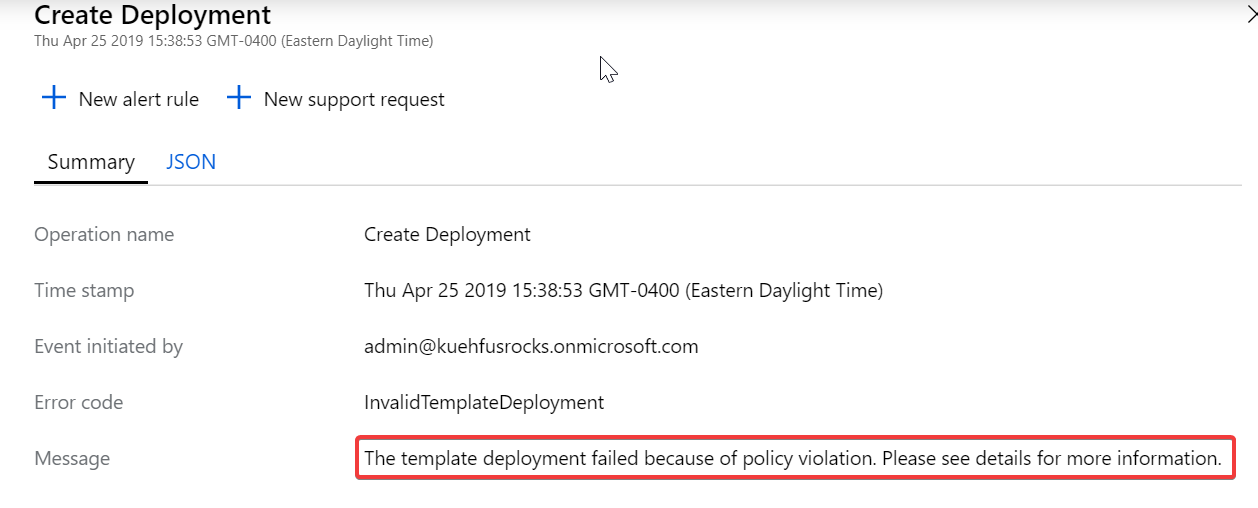
--name $VmName \

--image win2016datacenter \

--admin-username azureuser \

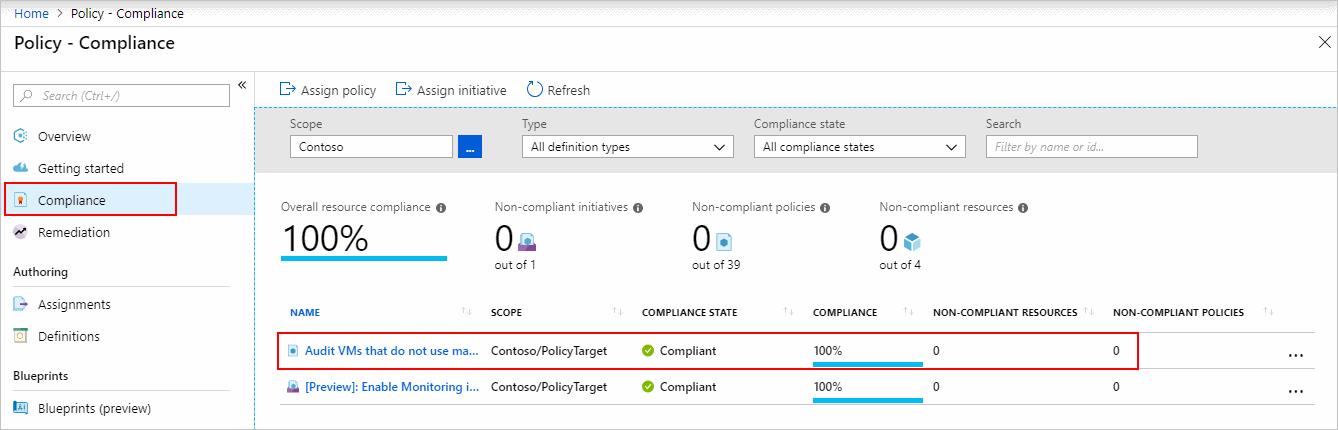
--admin-password $AdminPassword \

--size Standard\_GS1

* 1. Navigate to the Azure Activity Log and have a look at the message for why the deployment failed.  
       
     

Identify non-compliant resources

* 1. Select **Compliance** in the left side of the page. Then locate the **Audit VMs that do not use managed disks** policy assignment you created.



If there are any existing resources that aren't compliant with this new assignment, they appear under Non-compliant resources. When a condition is evaluated against your existing resources and found true, then those resources are marked as non-compliant with the policy. The following table shows how different policy effects work with the condition evaluation for the resulting compliance state. Although you don’t see the evaluation logic in the Azure portal, the compliance state results are shown. The compliance state result is either compliant or non-compliant.