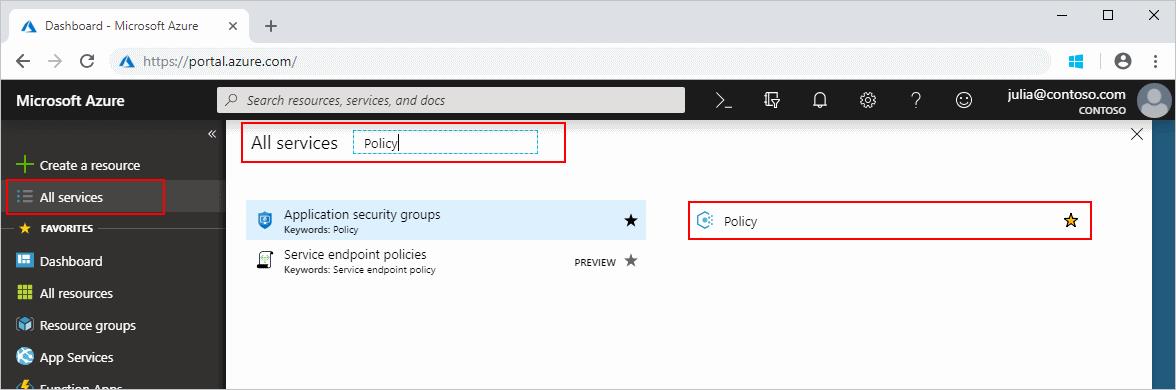
Create a policy assignment to identify non-compliant resources in your Azure environment

Scenario

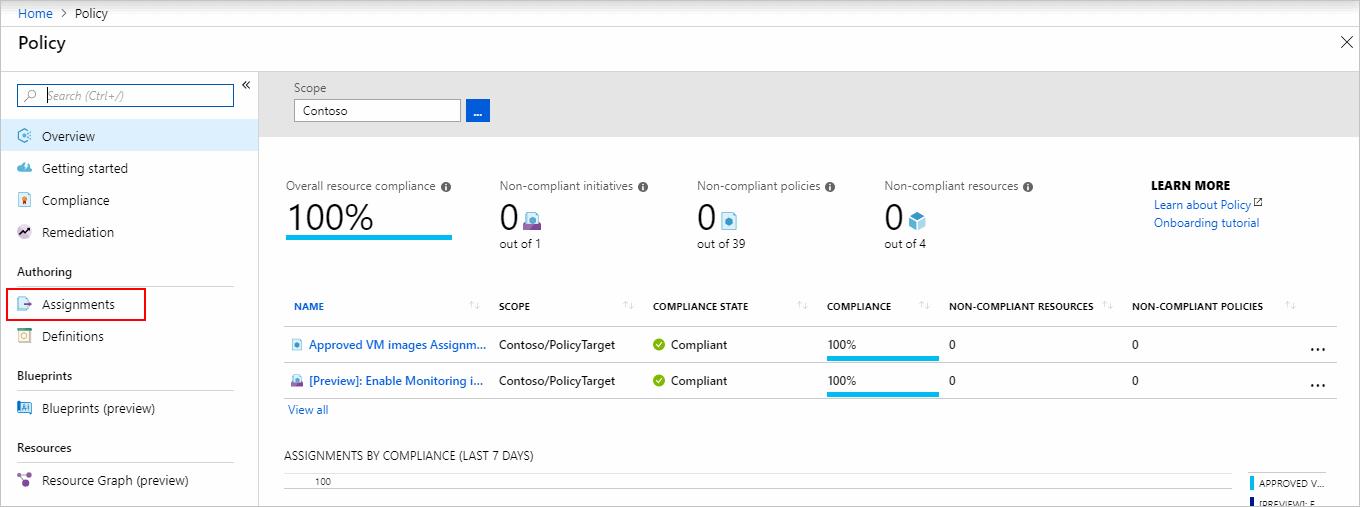
The first step in understanding compliance in Azure is to identify the status of your resources. This exercise steps you through the process of creating a policy assignment to identify virtual machines that aren't using managed disks. At the end of this process, you'll successfully identify virtual machines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

Create a policy assignment

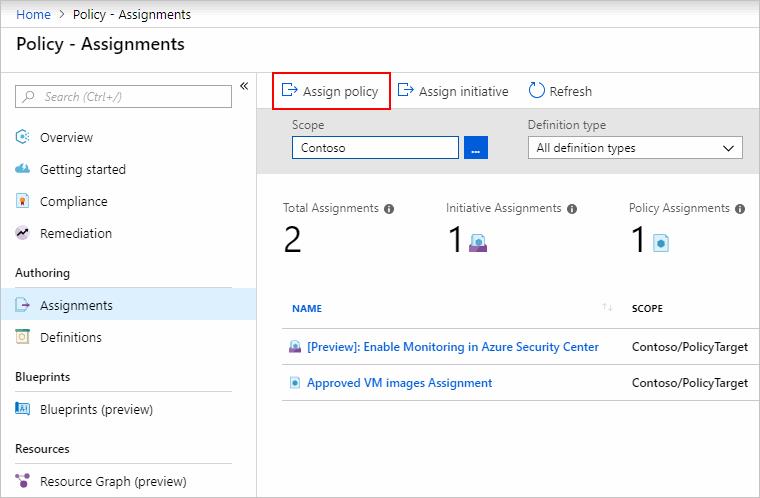
* 1. Launch the Azure Policy service in the Azure portal by clicking **All services**, then searching for and selecting Policy.



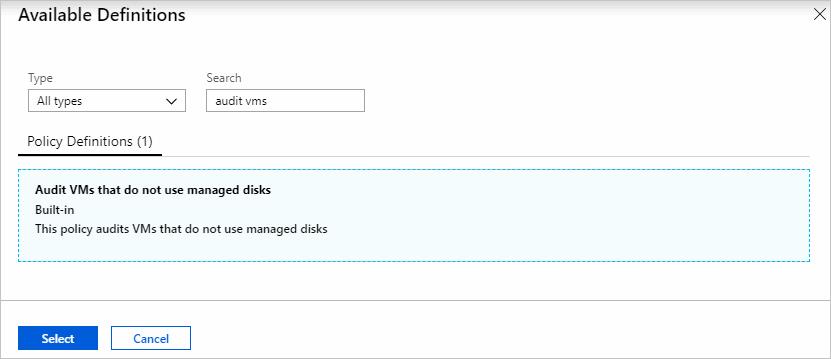
* 1. Select Assignments on the left side of the Azure Policy page. An assignment is a policy that has been assigned to take place within a specific scope.



* 1. Select **Assign Policy** from the top of the **Policy - Assignments** page.



* 1. On the **Assign Policy** page, select the Scope by clicking the ellipsis and selecting either a management group or subscription. Optionally, select a resource group. A scope determines what resources or grouping of resources the policy assignment gets enforced on. Then click **Select** at the bottom of the Scope page.
  2. 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.
  3. Select the Policy definition ellipsis to open the list of available definitions. Azure Policy comes with built-in policy definitions you can use.
  4. 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.



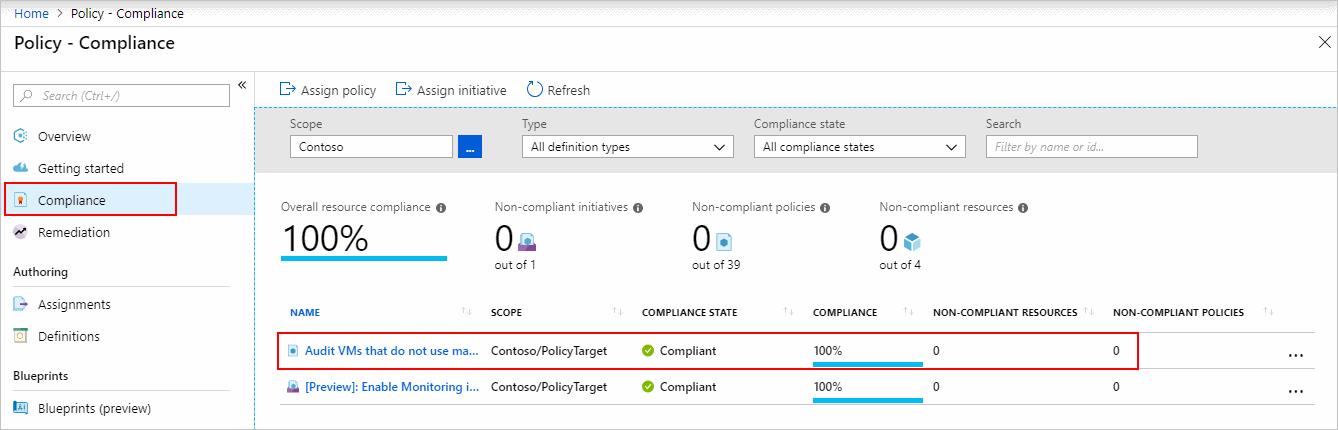
* 1. The **Assignment name** is automatically populated with the policy name you selected, but you can change it. For this example, leave *Audit VMs that do not use managed disks*. You can also add an optional **Description**. The description provides details about this policy assignment. **Assigned 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.

Identify non-compliant resources

**\*note, this could take up to 20min to show**

* 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.

# RBAC