Lab 02b - Manage Governance via Azure Policy Student lab manual

Lab scenario

In order to improve management of Azure resources in Contoso, you have been tasked with implementing the following functionality:

- tagging resource groups that include only infrastructure resources (such as Cloud Shell storage accounts)
- ensuring that only properly tagged infrastructure resources can be added to infrastructure resource groups
- remediating any non-compliant resources

Note: An **interactive lab simulation** is available that allows you to click through this lab at your own pace. You may find slight differences between the interactive simulation and the hosted lab, but the core concepts and ideas being demonstrated are the same.

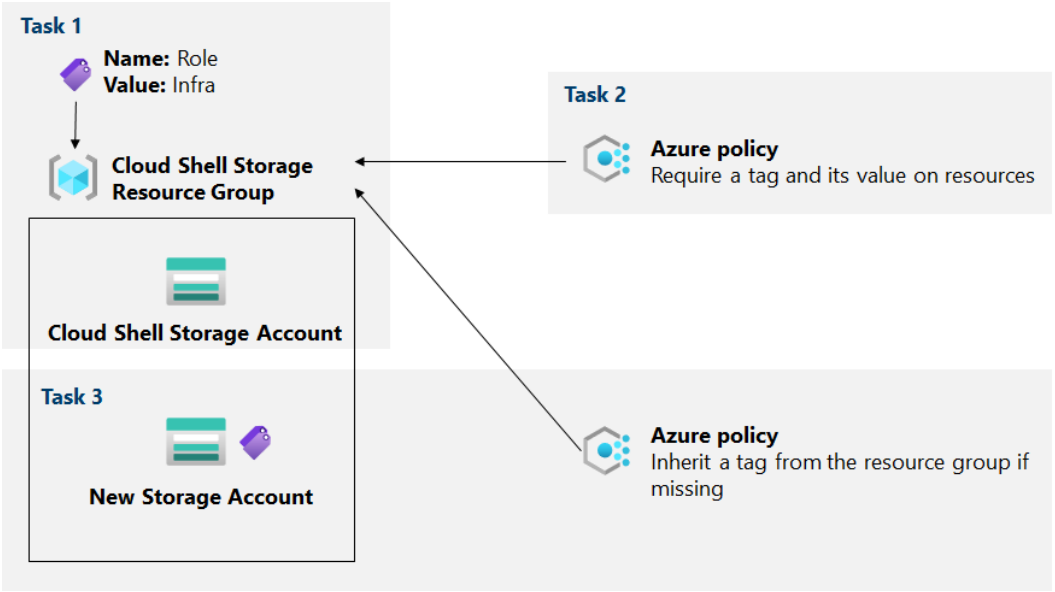
Objectives

In this lab, we will:

- Task 1: Create and assign tags via the Azure portal
- Task 2: Enforce tagging via an Azure policy
- Task 3: Apply tagging via an Azure policy

Estimated timing: 30 minutes

Architecture diagram



Instructions

Exercise 1

Task 1: Assign tags via the Azure portal

In this task, you will create and assign a tag to an Azure resource group via the Azure portal.

1. In the Azure portal, start a **PowerShell** session within the **Cloud Shell**.

   > **Note**: If this is the first time you are starting **Cloud Shell** and you are presented with the **You have no storage mounted** message, select the subscription you are using in this lab, and click **Create storage**.

2. From the Cloud Shell pane, run the following to identify the name of the storage account used by Cloud Shell:

   Code Copy

   ```
   df
   ```

3. In the output of the command, note the first part of the fully qualified path designating the Cloud Shell home drive mount (marked here as `xxxxxxxxxxxxx`:

   Code Copy

   ```
   //xxxxxxxxxxxxxx.file.core.windows.net/cloudshell   (..)  /usr/csuser/clouddrive
   ```

4. In the Azure portal, search and select **Storage accounts** and, in the list of the storage accounts, click the entry representing the storage account you identified in the previous step.

5. On the storage account blade, click the link representing the name of the resource group containing the storage account.

   Note: note what resource group the storage account is in, you'll need it later in the lab.

6. On the resource group blade, click Click **edit** next to **Tags** to create new tags.

7. Create a tag with the following settings and Apply your change:

Setting	Value
Name	**Role**
Value	**Infra**

8. Navigate back to the storage account blade. Review the **Overview** information and note that the new tag was not automatically assigned to the storage account.

Task 2: Enforce tagging via an Azure policy

In this task, you will assign the built-in *Require a tag and its value on resources* policy to the resource group and evaluate the outcome.

1. In the Azure portal, search for and select **Policy**.

2. In the **Authoring** section, click **Definitions**. Take a moment to browse through the list of built-in policy definitions that are available for you to use. List all built-in policies that involve the use of tags by selecting the **Tags** entry (and de-selecting all other entries) in the **Category** drop-down list.

3. Click the entry representing the **Require a tag and its value on resources** built-in policy and review its definition.

4. On the **Require a tag and its value on resources** built-in policy definition blade, click **Assign**.

5. Specify the **Scope** by clicking the ellipsis button and selecting the following values:

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab

Setting	Value
Resource Group	the name of the resource group containing the Cloud Shell account you identified in the previous task

> **Note**: A scope determines the resources or resource groups where the policy assignment takes effect. You could assign policies on the management group, subscription, or resource group level. You also have the option of specifying exclusions, such as individual subscriptions, resource groups, or resources (depending on the assignment scope).

6. Configure the **Basics** properties of the assignment by specifying the following settings (leave others with their defaults):

Setting	Value
Assignment name	**Require Role tag with Infra value**
Description	**Require Role tag with Infra value for all resources in the Cloud Shell resource group**
Policy enforcement	Enabled

> **Note**: The **Assignment name** is automatically populated with the policy name you selected, but you can change it. You can also add an optional **Description**. **Assigned by** is automatically populated based on the user name creating the assignment.

7. Click **Next** and set **Parameters** to the following values:

Setting	Value
Tag Name	**Role**
Tag Value	**Infra**

8. Click **Next** and review the **Remediation** tab. Leave the **Create a Managed Identity** checkbox unchecked.

> **Note**: This setting can be used when the policy or initiative includes the **deployIfNotExists** or **Modify** effect.

9. Click **Review + Create** and then click **Create**.

> **Note**: Now you will verify that the new policy assignment is in effect by attempting to create another Azure Storage account in the resource group without explicitly adding the required tag.

> **Note**: It might take between 5 and 15 minutes for the policy to take effect.

10. Navigate back to the blade of the resource group hosting the storage account used for the Cloud Shell home drive, which you identified in the previous task.

11. On the resource group blade, click **+ Create** and then search for **Storage Account**, and click **+ Create**.

12. On the **Basics** tab of the **Create storage account** blade, verify that you are using the Resource Group that the Policy was applied to and specify the following settings (leave others with their defaults), click **Review + create** and then click **Create**:

Setting	Value
Storage account name	any globally unique combination of between 3 and 24 lower case letters and digits, starting with a letter

13. Once you create the deployment, you should see the **Deployment failed** message in the **Notifications** list of the portal. From the **Notifications** list, navigate to the deployment overview and click the **Deployment failed. Click here for details** message to identify the reason for the failure.

> **Note**: Verify whether the error message states that the resource deployment was disallowed by the policy.

> **Note**: By clicking the **Raw Error** tab, you can find more details about the error, including the name of the role definition **Require Role tag with Infra value**. The deployment failed because the storage account you attempted to create did not have a tag named **Role** with its value set to **Infra**.

Task 3: Apply tagging via an Azure policy

In this task, we will use a different policy definition to remediate any non-compliant resources.

1. In the Azure portal, search for and select **Policy**.
2. In the **Authoring** section, click **Assignments**.
3. In the list of assignments, click the ellipsis icon in the row representing the **Require Role tag with Infra value** policy assignment and use the **Delete assignment** menu item to delete the assignment.
4. Click **Assign policy** and specify the **Scope** by clicking the ellipsis button and selecting the following values:

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource Group	the name of the resource group containing the Cloud Shell account you identified in the first task

5. To specify the **Policy definition**, click the ellipsis button and then search for and select **Inherit a tag from the resource group if missing**.
6. Configure the remaining **Basics** properties of the assignment by specifying the following settings (leave others with their defaults):

Setting	Value
Assignment name	**Inherit the Role tag and its Infra value from the Cloud Shell resource group if missing**
Description	**Inherit the Role tag and its Infra value from the Cloud Shell resource group if missing**
Policy enforcement	Enabled

7. Click **Next** and set **Parameters** to the following values:

Setting	Value
Tag Name	**Role**

8. Click **Next** and, on the **Remediation** tab, configure the following settings (leave others with their defaults):

Setting	Value
Create a remediation task	enabled
Policy to remediate	**Inherit a tag from the resource group if missing**

> **Note**: This policy definition includes the **Modify** effect.

9. Click **Review + Create** and then click **Create**.

> **Note**: To verify that the new policy assignment is in effect, you will create another Azure Storage account in the same resource group without explicitly adding the required tag.

> **Note**: It might take between 5 and 15 minutes for the policy to take effect.

10. Navigate back to the blade of the resource group hosting the storage account used for the Cloud Shell home drive, which you identified in the first task.
11. On the resource group blade, click **+ Create** and then search for **Storage Account**, and click **+ Create**.
12. On the **Basics** tab of the **Create storage account** blade, verify that you are using the Resource Group that the Policy was applied to and specify the following settings (leave others with their defaults) and click **Review + create**:

Setting	Value
Storage account name	any globally unique combination of between 3 and 24 lower case letters and digits, starting with a letter

13. Verify that this time the validation passed and click **Create**.
14. Once the new storage account is provisioned, click **Go to resource** button and, on the **Overview** blade of the newly created storage account, note that the tag **Role** with the value **Infra** has been automatically assigned to the resource.

Task 4: Clean up resources

> **Note**: Remember to remove any newly created Azure resources that you no longer use. Removing unused resources ensures you will not see unexpected charges, although keep in mind that Azure policies do not incur extra cost.

> **Note**: Don't worry if the lab resources cannot be immediately removed. Sometimes resources have dependencies and take a longer time to delete. It is a common Administrator task to monitor resource usage, so just periodically review your resources in the Portal to see how the cleanup is going.

1. In the portal, search for and select **Policy**.
2. In the **Authoring** section, click **Assignments**, click the ellipsis icon to the right of the assignment you created in the previous task and click **Delete assignment**.
3. In the portal, search for and select **Storage accounts**.
4. In the list of storage accounts, select the resource group corresponding to the storage account you created in the last task of this lab. Select **Tags** and click **Delete** (Trash can to the right) to the **Role:Infra** tag and press **Apply**.
5. Click **Overview** and click **Delete** on the top of the storage account blade. When prompted for the confirmation, in the **Delete storage account** blade, type the name of the storage account to confirm and click **Delete**.

Review

In this lab, you have:

- Created and assigned tags via the Azure portal
- Enforced tagging via an Azure policy
- Applied tagging via an Azure policy