**Module 2: Governance and Compliance**

**Exercise 1: Manage Subscriptions and RBAC**

#### Task 1: Implement Management Groups

In this task, you will create and configure management groups.

1. Sign in to the [Azure portal](https://portal.azure.com/).
2. Search for and select **Management groups** and then, on the **Management groups** blade, click **+ Add management group**.

**Note**: If you have not previously created Management Groups, select **Start using Management Groups**

1. Create a management group with the following settings:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Management group ID | **az104-02-mg1** |
| Management group display name | **az104-02-mg1** |

1. In the list of management groups, click the entry representing the newly created management group and then display its **details**.
2. From the **az104-02-mg1** blade, click **+ Add subscription** and add the subscription you are using in this lab to the management group.

**Note**: Copy the ID of your Azure subscription into Clipboard. You will need it in the next task.

#### Task 2: Create custom RBAC roles

In this task, you will create a definition of a custom RBAC role.

1. From the lab computer, open the file **az104-02a-customRoleDefinition.json** in Notepad and review its content:
2. Replace the SUBSCRIPTION\_ID placeholder in the JSON file with the subscription ID you copied into Clipboard and save the change.
3. In the Azure portal, open **Cloud Shell** pane by clicking on the toolbar icon directly to the right of the search textbox.
4. If prompted to select either **Bash** or **PowerShell**, select **PowerShell**.

**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**.

1. In the toolbar of the Cloud Shell pane, click the **Upload/Download files** icon, in the drop-down menu click **Upload**, and upload the file **az104-02a-customRoleDefinition.json** into the Cloud Shell home directory.
2. From the Cloud Shell pane, run the following to create the custom role definition:

*New-AzRoleDefinition -InputFile $HOME/az104-02a-customroledefinition.json*

*New-AzRoleDefinition -InputFile $HOME/customroledefinition.json*

1. Close the Cloud Shell pane.

#### Task 3: Assign RBAC roles

In this task, you will create an Azure Active Directory user, assign the RBAC role you created in the previous task to that user, and verify that the user can perform the task specified in the RBAC role definition.

1. In the Azure portal, search for and select **Azure Active Directory**, on the Azure Active Directory blade, click **Users**, and then click **+ New user**.
2. Create a new user with the following settings (leave others with their defaults):

|  |  |
| --- | --- |
| **Setting** | **Value** |
| User name | **az104-02-aaduser1** |
| Name | **az104-02-aaduser1** |
| Let me create the password | **enabled** |
| Initial password | **Pa55w.rd124** |

**Note**: **Copy to clipboard** the full **User name**. You will need it later in this lab.

1. In the Azure portal, navigate back to the **az104-02-mg1** management group and display its **details**.
2. Click **Access control (IAM)**, click **+ Add** followed by **Role assignment**, and assign the **Support Req. Contributor (Custom)** role to the newly created user account.
3. Open an **InPrivate** browser window and sign in to the [Azure portal](https://portal.azure.com/) using the newly created user account. When prompted to update the password, change the password for the user.

**Note**: Rather than typing the user name, you can paste the content of Clipboard.

1. In the **InPrivate** browser window, in the Azure portal, search and select **Resource groups** to verify that the az104-02-aaduser1 user can see all resource groups.
2. In the **InPrivate** browser window, in the Azure portal, search and select **All resources** to verify that the az104-02-aaduser1 user cannot see any resources.
3. In the **InPrivate** browser window, in the Azure portal, search and select **Help + support** and then click **+ New support request**.
4. In the **InPrivate** browser window, on the **Basic** tab of the **Help + support - New support request** blade, select the **Service and subscription limits (quotas)** issue type and note that the subscription you are using in this lab is listed in the **Subscription** drop-down list.

**Note**: The presence of the subscription you are using in this lab in the **Subscription** drop-down list indicates that the account you are using has the permissions required to create the subscription-specific support request.

**Note**: If you do not see the **Service and subscription limits (quotas)** option, sign out from the Azure portal and sign in back.

1. Do not continue with creating the support request. Instead, sign out as the az104-02-aaduser1 user from the Azure portal and close the InPrivate browser window.

#### Clean up resources

**Note**: Remember to remove any newly created Azure resources that you no longer use.

**Note**: Removing unused resources ensures you will not see unexpected charges, although, resources created in this lab do not incur extra cost.

1. In the Azure portal, search for and select **Azure Active Directory**, on the Azure Active Directory blade, click **Users**.
2. On the **Users - All users** blade, click **az104-02-aaduser1**.
3. On the **az104-02-aaduser1 - Profile** blade, copy the value of **Object ID** attribute.
4. In the Azure portal, start a **PowerShell** session within the **Cloud Shell**.
5. From the Cloud Shell pane, run the following to remove the assignment of the custom role definition (replace the [object\_ID] placeholder with the value of the **object ID** attribute of the **az104-02-aaduser1** Azure Active Directory user account you copied earlier in this task):

*$scope = (Get-AzRoleAssignment -RoleDefinitionName 'Support Request Contributor (Custom)').Scope*

*Remove-AzRoleAssignment -ObjectId '[object\_ID]' -RoleDefinitionName 'Support Request Contributor (Custom)' -Scope $scope*

1. From the Cloud Shell pane, run the following to remove the custom role definition:

*Remove-AzRoleDefinition -Name 'Support Request Contributor (Custom)' -Force*

1. In the Azure portal, navigate back to the **Users - All users** blade of the **Azure Active Directory**, and delete the **az104-02-aaduser1** user account.
2. In the Azure portal, navigate to the **az104-02-mg1** management group and display its **details**.
3. Right-click the **ellipsis** icon to the right of the entry representing your Azure subscription and click **Move**.
4. On the **Move** blade, select the management group which the subscription was originally part of and click **Save**.
5. Navigate back to the **Management groups** blade, right click the **ellipsis** icon to the right of the **az104-02-mg1** management group and click **Delete**.

**Exercise 2: Manage Governance via Azure Policy**

#### 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**.

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

*df*

1. 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 xxxxxxxxxxxxxx:

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

1. 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.
2. On the storage account blade, click the link representing the name of the resource group containing the storage account.
3. On the resource group blade, click **Tags**.
4. Create a tag with the following settings and save your change:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Name | **Role** |
| Value | **Infra** |

1. 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** |
| 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).

1. 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.

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

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Tag Name | **Role** |
| Tag Value | **Infra** |

1. 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.

1. 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.

1. 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.
2. On the resource group blade, click **+ Add**.
3. On the **New** blade, search for and select **Storage account**, and click **Create**.
4. On the **Basics** tab of the **Create storage account** blade, 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** |

1. Note that the validation failed. Click the link **Validation failed. Click here to view details** to display the **Errors** blade and identify the reason for the failure.

**Note**: 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**.