



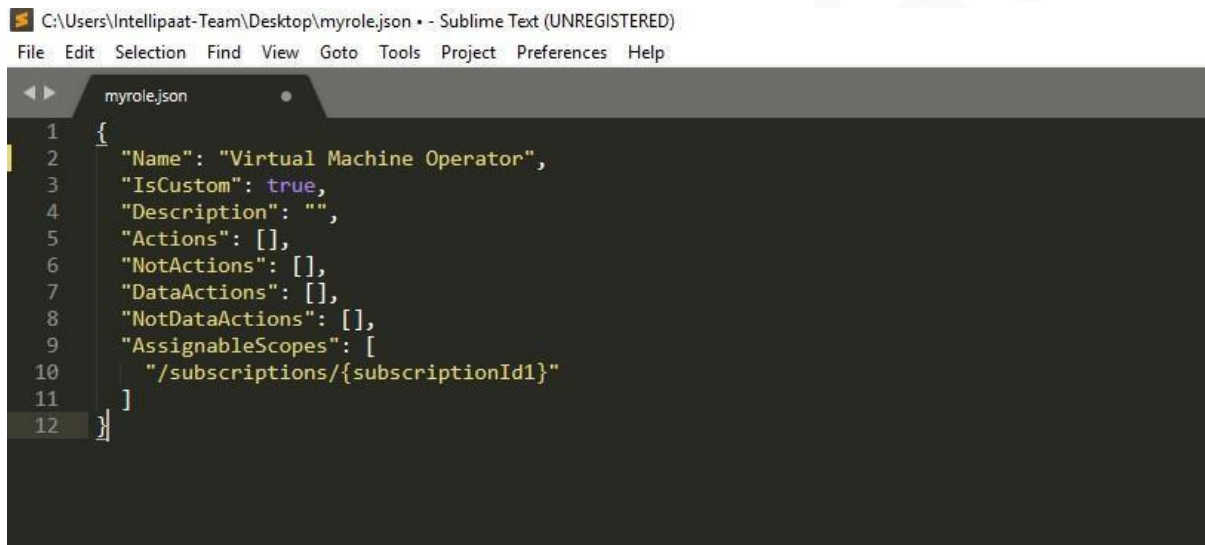
Module 8: Hands-On: Create a Custom Role Using Azure CLI

Go to the following link and copy the custom role example JSON template and create a JSON file with this code. Name this file as template.json

<https://docs.microsoft.com/en-us/azure/role-based-access-control/tutorial-custom-role-cli#create-a-custom-role>

Note: We will edit this JSON template and define our own custom role with its custom permissions. The custom role that we will create will be called Virtual Machine Operator. This role will allow the user to start, stop or monitor VMs.

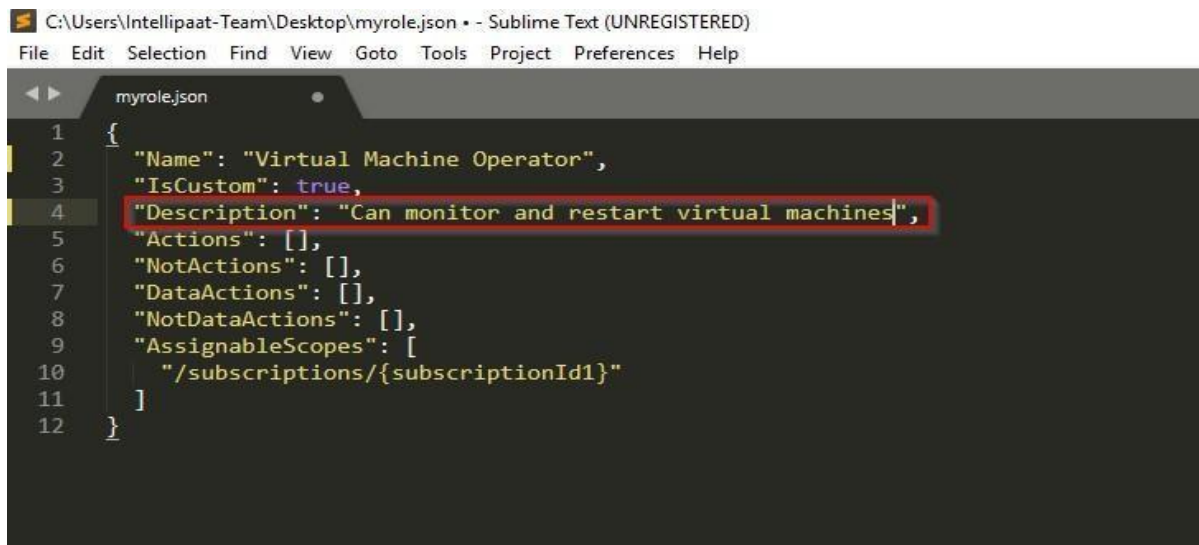
Open your JSON file in an editor and in the name field, provide the name of your custom role as “Virtual Machine Operator”



```
C:\Users\IntelliPaat-Team\Desktop\myrole.json - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help

myrole.json
1 {
2   "Name": "Virtual Machine Operator",
3   "IsCustom": true,
4   "Description": "",
5   "Actions": [],
6   "NotActions": [],
7   "DataActions": [],
8   "NotDataActions": [],
9   "AssignableScopes": [
10    "/subscriptions/{subscriptionId}"
11  ]
12 }
```

In the description field, give the description for your custom role as “Can monitor and restart virtual machines”



```
C:\Users\IntelliPaat-Team\Desktop\myrole.json - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help

myrole.json
1 {
2   "Name": "Virtual Machine Operator",
3   "IsCustom": true,
4   "Description": "Can monitor and restart virtual machines",
5   "Actions": [],
6   "NotActions": [],
7   "DataActions": [],
8   "NotDataActions": [],
9   "AssignableScopes": [
10    "/subscriptions/{subscriptionId}"
11  ]
12 }
```

In the actions field, you define the operations that this role is allowed to do. Assign the following information in your actions field

```
"Microsoft.Storage/*/read",

"Microsoft.Network/*/read",

"Microsoft.Compute/*/read",

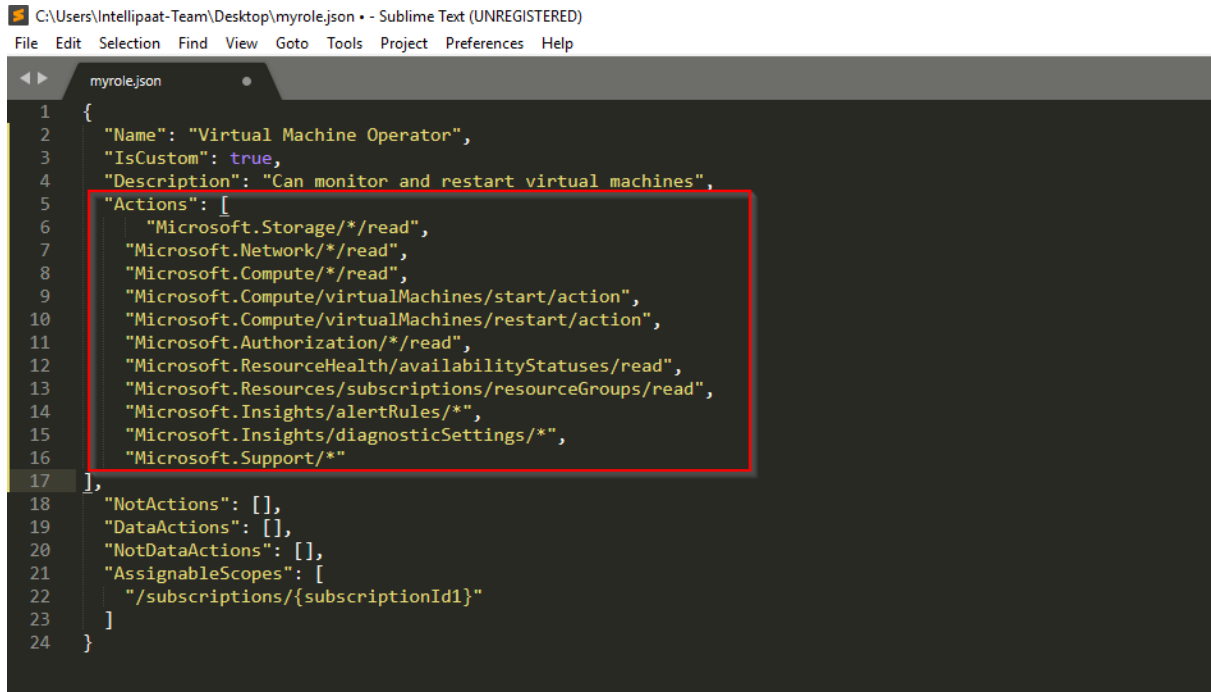
"Microsoft.Compute/virtualMachines/start/action",

"Microsoft.Compute/virtualMachines/restart/action",

"Microsoft.Authorization/*/read",

"Microsoft.ResourceHealth/availab
```

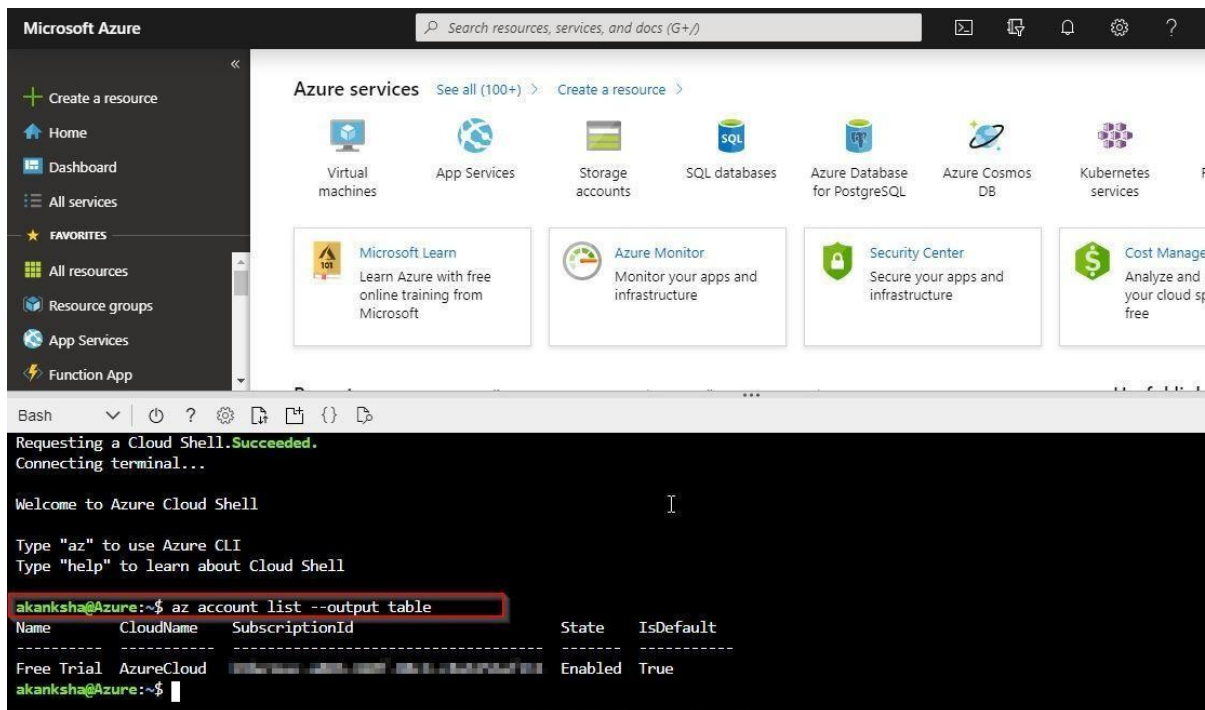
To learn about more actions that can be used, visit the following link:
<https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftcompute>



```
1 {
2   "Name": "Virtual Machine Operator",
3   "IsCustom": true,
4   "Description": "Can monitor and restart virtual machines",
5   "Actions": [
6     "Microsoft.Storage/*/read",
7     "Microsoft.Network/*/read",
8     "Microsoft.Compute/*/read",
9     "Microsoft.Compute/virtualMachines/start/action",
10    "Microsoft.Compute/virtualMachines/restart/action",
11    "Microsoft.Authorization/*/read",
12    "Microsoft.ResourceHealth/availabilityStatuses/read",
13    "Microsoft.Resources/subscriptions/resourceGroups/read",
14    "Microsoft.Insights/alertRules/*",
15    "Microsoft.Insights/diagnosticSettings/*",
16    "Microsoft.Support/*"
17  ],
18  "NotActions": [],
19  "DataActions": [],
20  "NotDataActions": [],
21  "AssignableScopes": [
22    "/subscriptions/{subscriptionId}"
23  ]
24 }
```

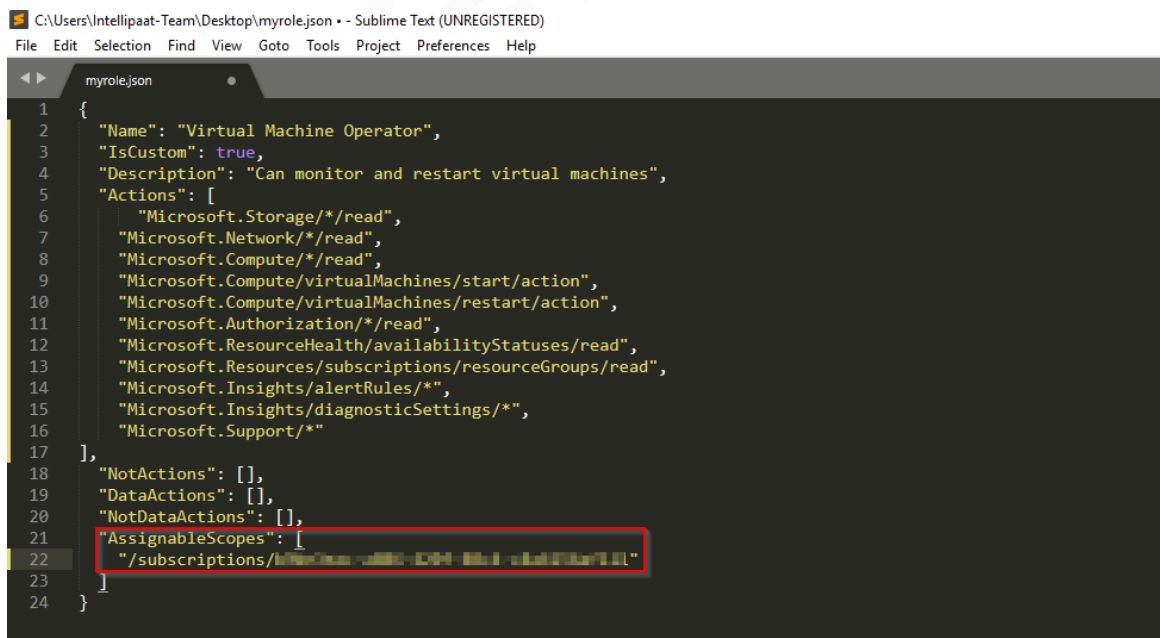
In the assignable scopes field, you have to provide your subscription ID. You can get the subscription ID using the following command in your CLI (launch CLI from your portal):

az account list - output table



The screenshot shows the Microsoft Azure portal interface. At the bottom, the Azure Cloud Shell is open, displaying the command `az account list --output table` and its output. The output is a table with the following columns: Name, CloudName, SubscriptionId, State, and IsDefault.

Name	CloudName	SubscriptionId	State	IsDefault
Free Trial	AzureCloud	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx	Enabled	True



The screenshot shows a Sublime Text editor window with a file named `myrole.json`. The JSON content is as follows:

```

{
  "Name": "Virtual Machine Operator",
  "IsCustom": true,
  "Description": "Can monitor and restart virtual machines",
  "Actions": [
    "Microsoft.Storage/*/read",
    "Microsoft.Network/*/read",
    "Microsoft.Compute/*/read",
    "Microsoft.Compute/virtualMachines/start/action",
    "Microsoft.Compute/virtualMachines/restart/action",
    "Microsoft.Authorization/*/read",
    "Microsoft.ResourceHealth/availabilityStatuses/read",
    "Microsoft.Resources/subscriptions/resourceGroups/read",
    "Microsoft.Insights/alertRules/*",
    "Microsoft.Insights/diagnosticSettings/*",
    "Microsoft.Support/*"
  ],
  "NotActions": [],
  "DataActions": [],
  "NotDataActions": [],
  "AssignableScopes": [
    "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
  ]
}

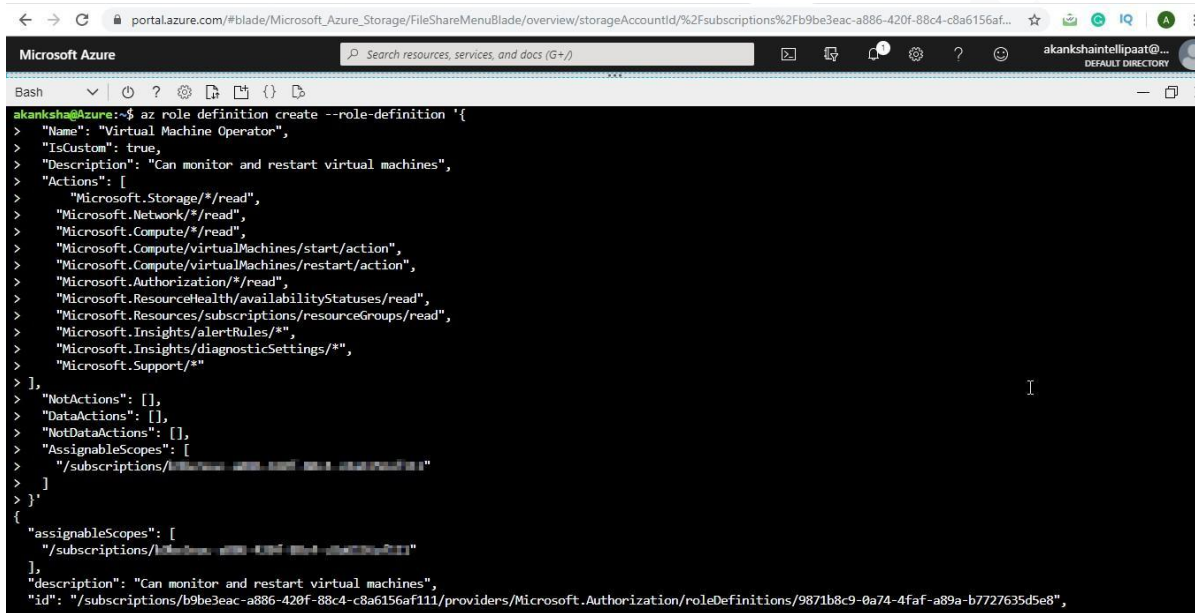
```

The `AssignableScopes` field is highlighted with a red box, showing a single subscription ID.

Save all the changes made to the JSON file. Go to Azure CLI and run the following command to create the custom role.

az role definition update - role-definition 'JSON script'

Note: Replace JSON script with your template.json script as shown in the following screenshot.



```
akanksha@Azure:~$ az role definition create --role-definition '{
>   "Name": "Virtual Machine Operator",
>   "IsCustom": true,
>   "Description": "Can monitor and restart virtual machines",
>   "Actions": [
>     "Microsoft.Storage/*/*/*",
>     "Microsoft.Network/*/*/*",
>     "Microsoft.Compute/*/*/*",
>     "Microsoft.Compute/virtualMachines/start/action",
>     "Microsoft.Compute/virtualMachines/restart/action",
>     "Microsoft.Authorization/*/*/*",
>     "Microsoft.ResourceHealth/availabilityStatuses/read",
>     "Microsoft.Resources/subscriptions/resourceGroups/read",
>     "Microsoft.Insights/alertRules/*/*",
>     "Microsoft.Insights/diagnosticSettings/*/*",
>     "Microsoft.Support/*/*/*"
>   ],
>   "NotActions": [],
>   "DataActions": [],
>   "NotDataActions": [],
>   "AssignableScopes": [
>     "/subscriptions/1b9b3eac-a886-420f-88c4-c8a6156af111"
>   ]
> }'
```

The screenshot shows a terminal window with the Azure CLI command `az role definition create --role-definition '{ ... }'` being executed. The command creates a custom role named "Virtual Machine Operator" with specific permissions. The terminal output shows the command being executed and the role definition being created.

The new custom role is now available and can be assigned to users, groups, or service principals just like built-in roles.