# Azure Managing RBAC

# 

## **Tutorial**

In this tutorial, we are going to:

1. Create a custom role called *VM Operator*, which allows the user to monitor and restart virtual machines inside our subscription.
2. Change the scope of the role to one resource group in the subscription
3. Delete the custom role
4. Create a new json file called *vm-operator.json*:

**$ cd**

**$ touch vm-operator.json**

1. Use a text editor, such as vim or nano, to enter the following into this file:

{

"Name": "",

"IsCustom": true,

"Description": "",

"Actions": [],

"NotActions": [],

"DataActions": [],

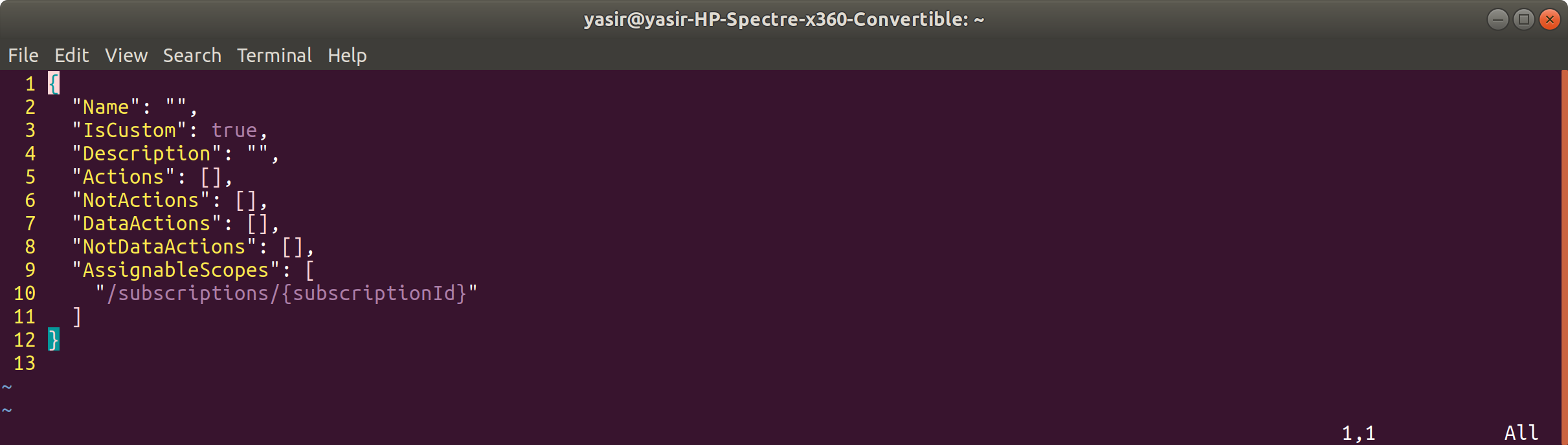
"NotDataActions": [],

"AssignableScopes": [

"/subscriptions/{subscriptionId}"

]

}



1. In the Actions property, add:

"Microsoft.Storage/\*/read",

"Microsoft.Network/\*/read",

"Microsoft.Compute/\*/read",

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

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

"Microsoft.Authorization/\*/read",

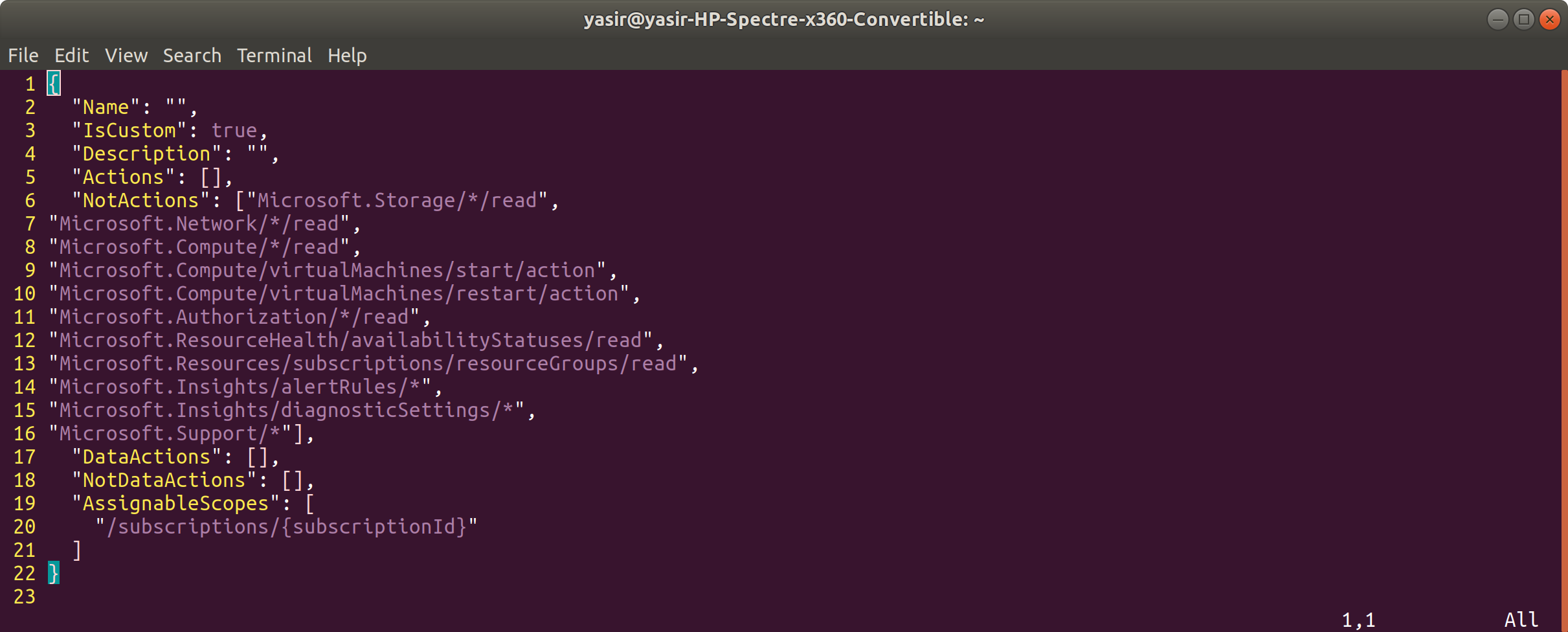
"Microsoft.ResourceHealth/availabilityStatuses/read",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Insights/alertRules/\*",

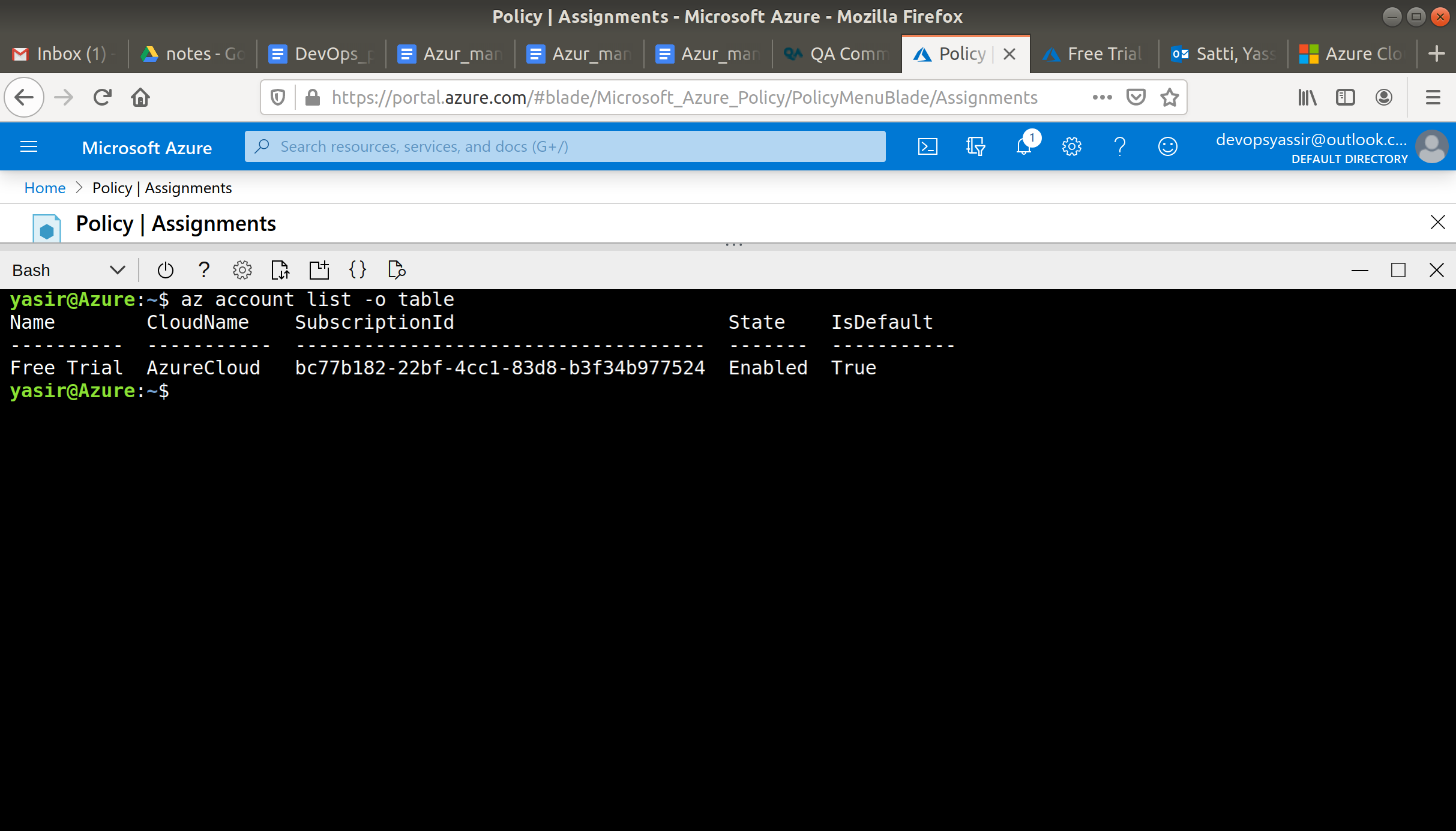
"Microsoft.Insights/diagnosticSettings/\*",

"Microsoft.Support/\*"



1. In AssignableScopes, replace {subscriptionID} with your subscription id. You can find this using:

**$ az account list -o table**

****

1. Change the Name property to “Virtual Machine Operator” and the Description property to “Can monitor and restart virtual machines”.
2. Your json should look like this:

{

"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": [],

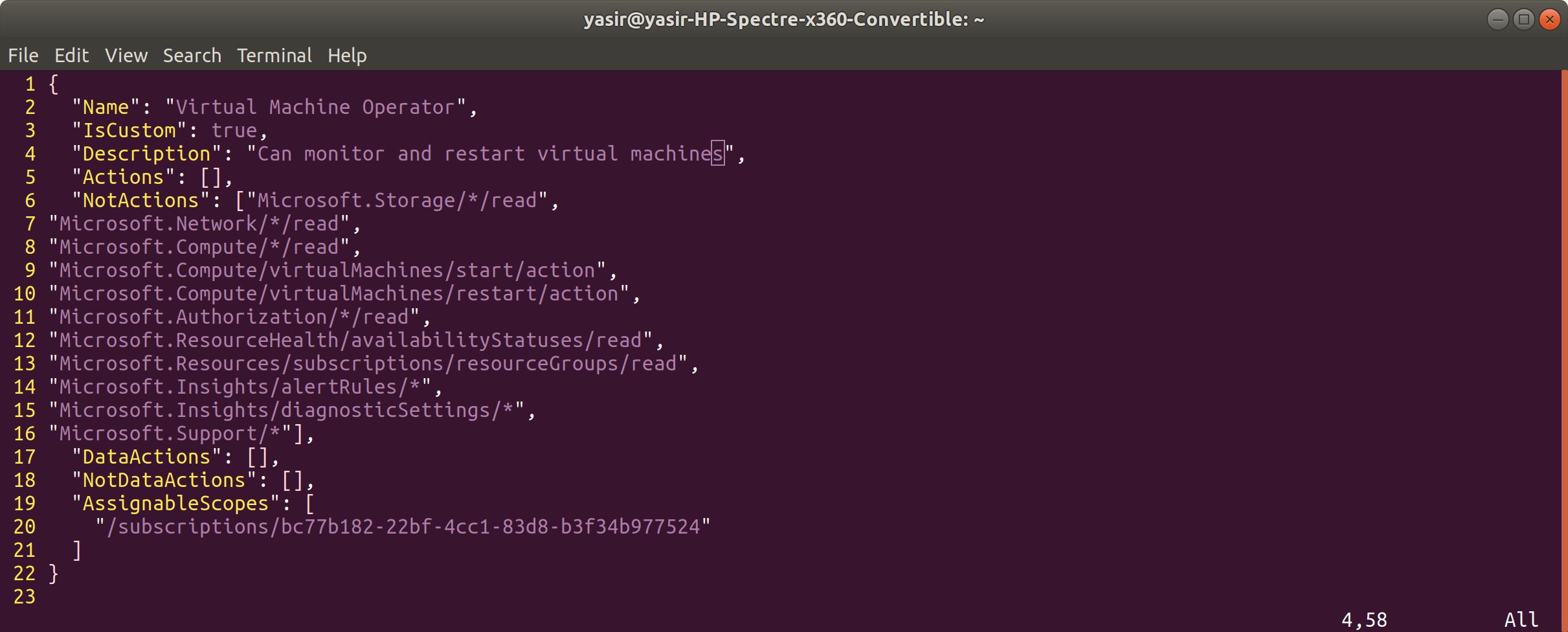
"NotDataActions": [],

"AssignableScopes": [

"/subscriptions/00000000-0000-0000-0000-000000000000"

]

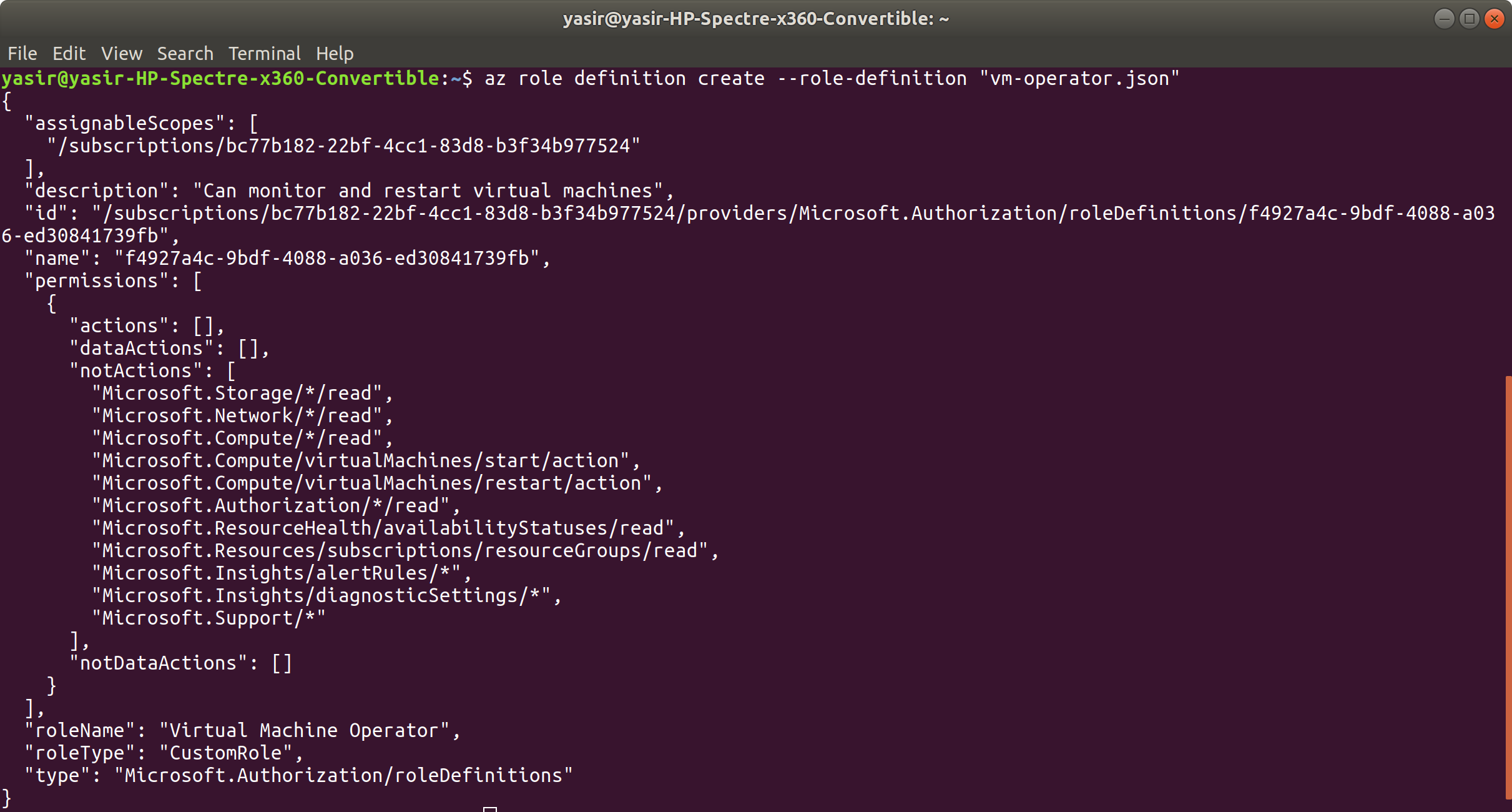
}



1. Create the custom role on Azure:

**az role definition create --role-definition "vm-operator.json"**

**The role is now available and can be assigned!**

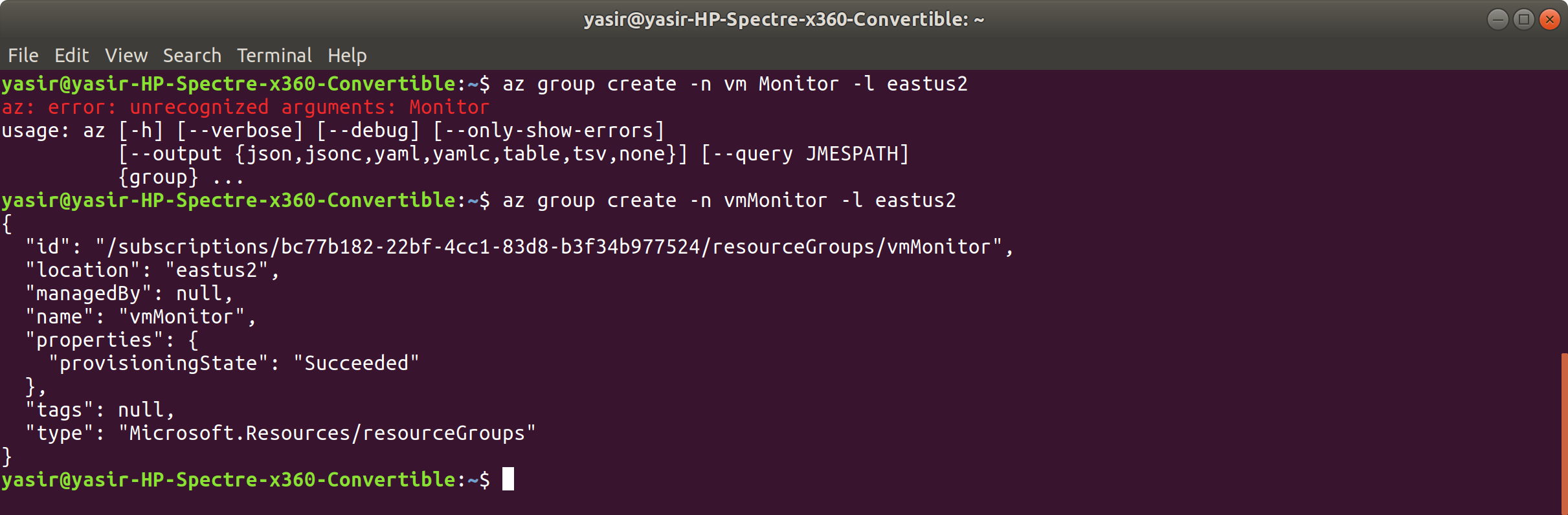
****

1. You can list all of your custom roles using:

**az role definition list --custom-role-only true**

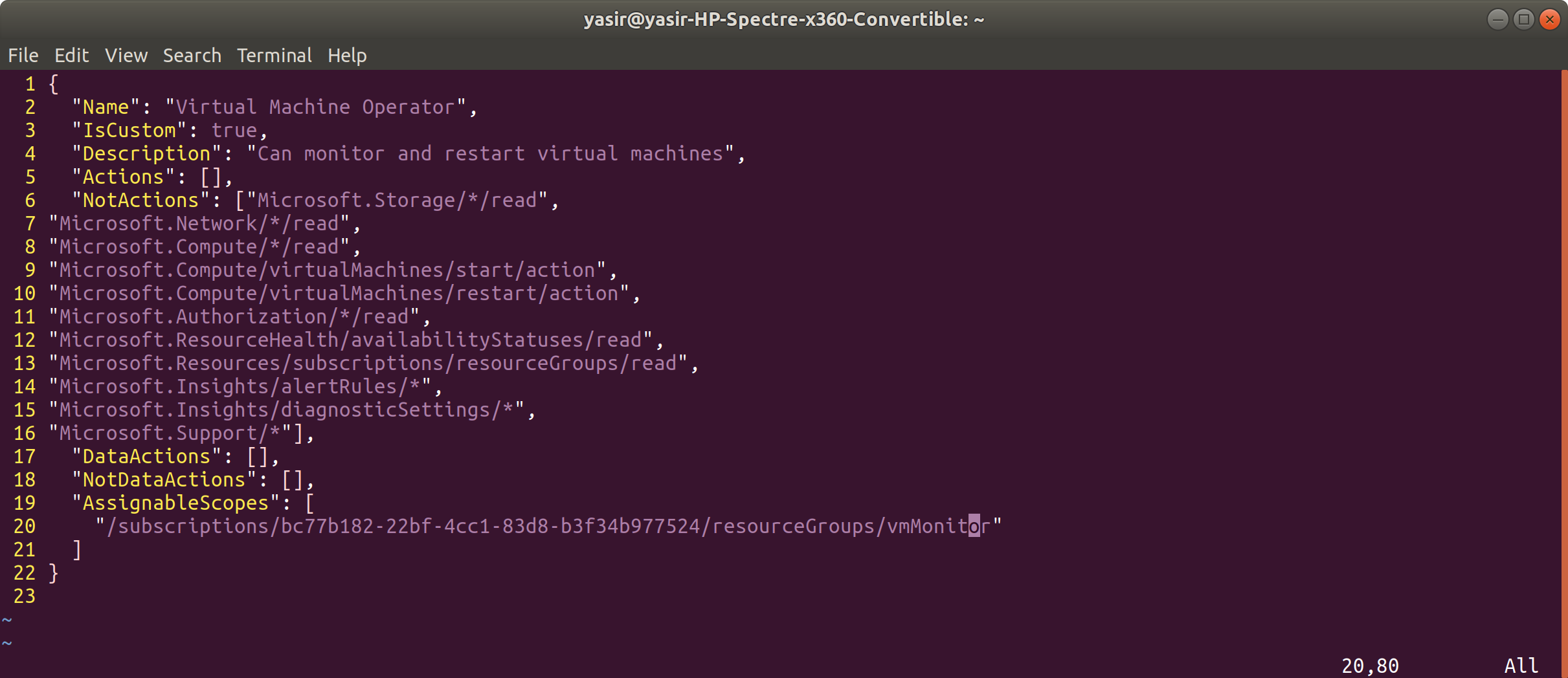
1. Create a resource group:

**az group create -n vmMonitor -l uksouth**

****

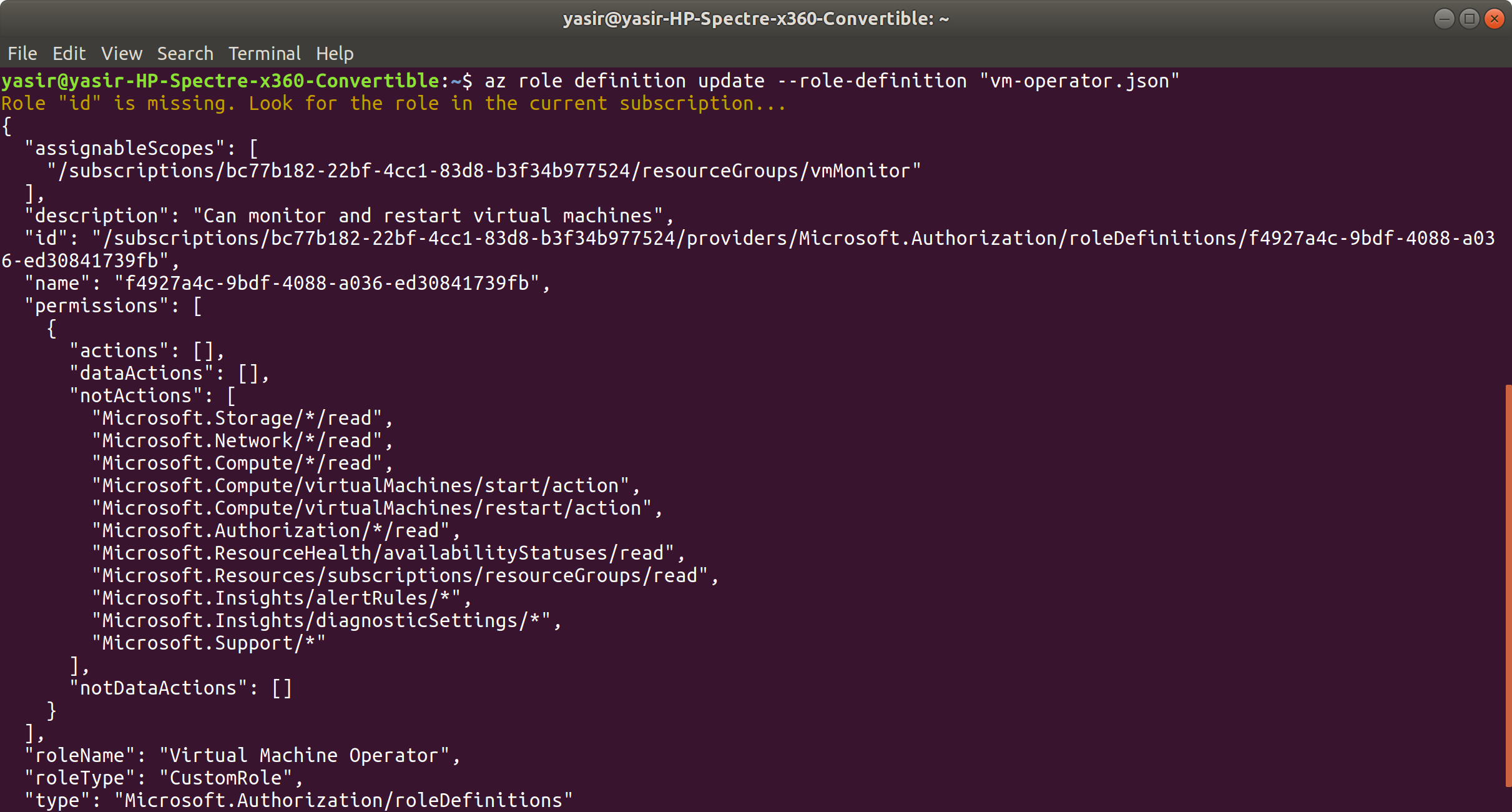
1. We now want to change the custom role so that the scope is the resource group we just created, rather than the whole subscription. Change the AssingableScopes property in your json file to:

"/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/vmMonitor"

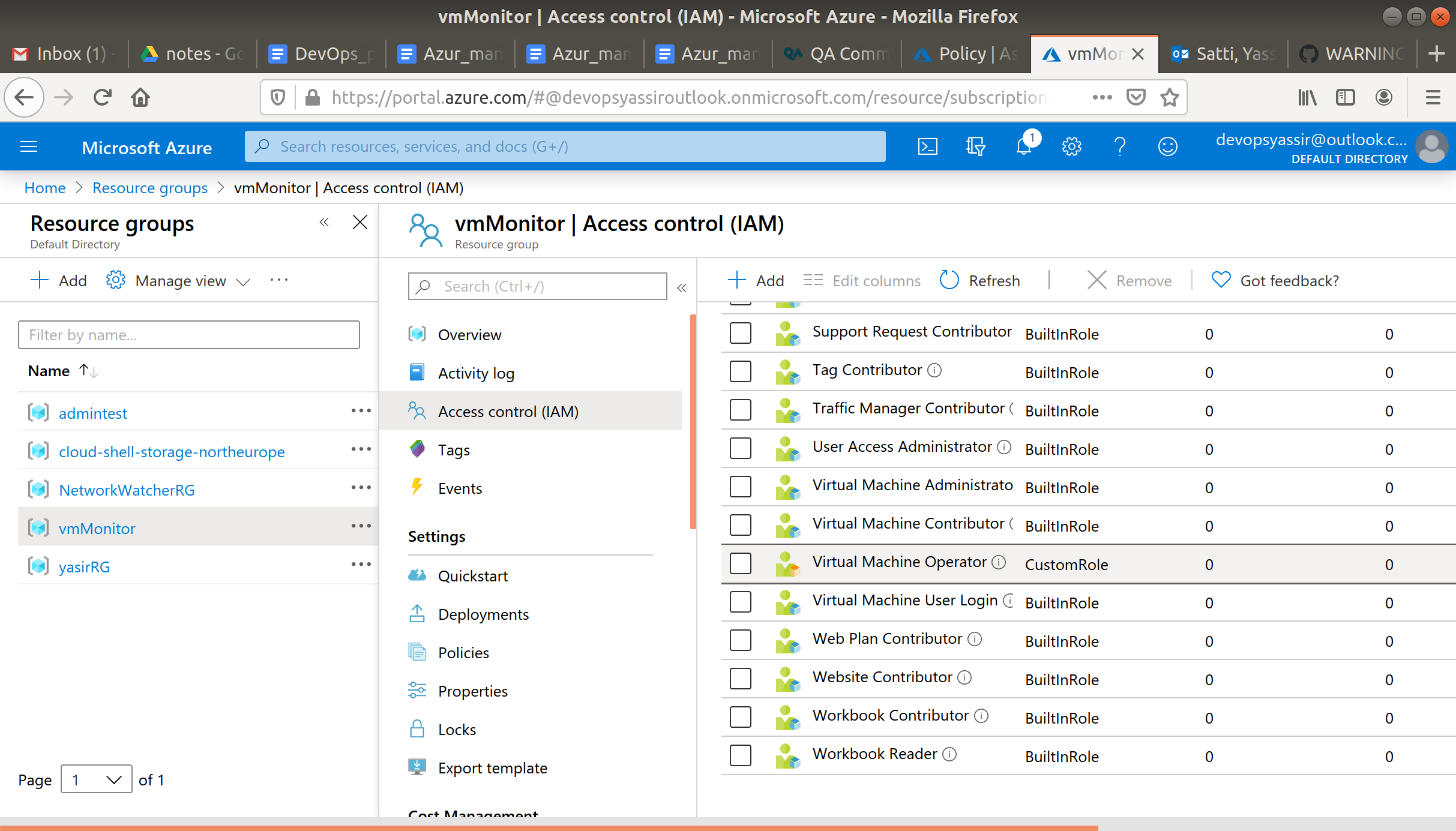


1. Update the role with:

**az role definition update --role-definition "vm-operator.json"**

****

1. Go to the Azure Portal:  
   * Search Resource groups and click on it when it appears
   * Click on the vmMonitor resource group and then Access control (IAM) on the left hand side
   * Click on Roles and in this list, you should see Virtual Machine Operator:



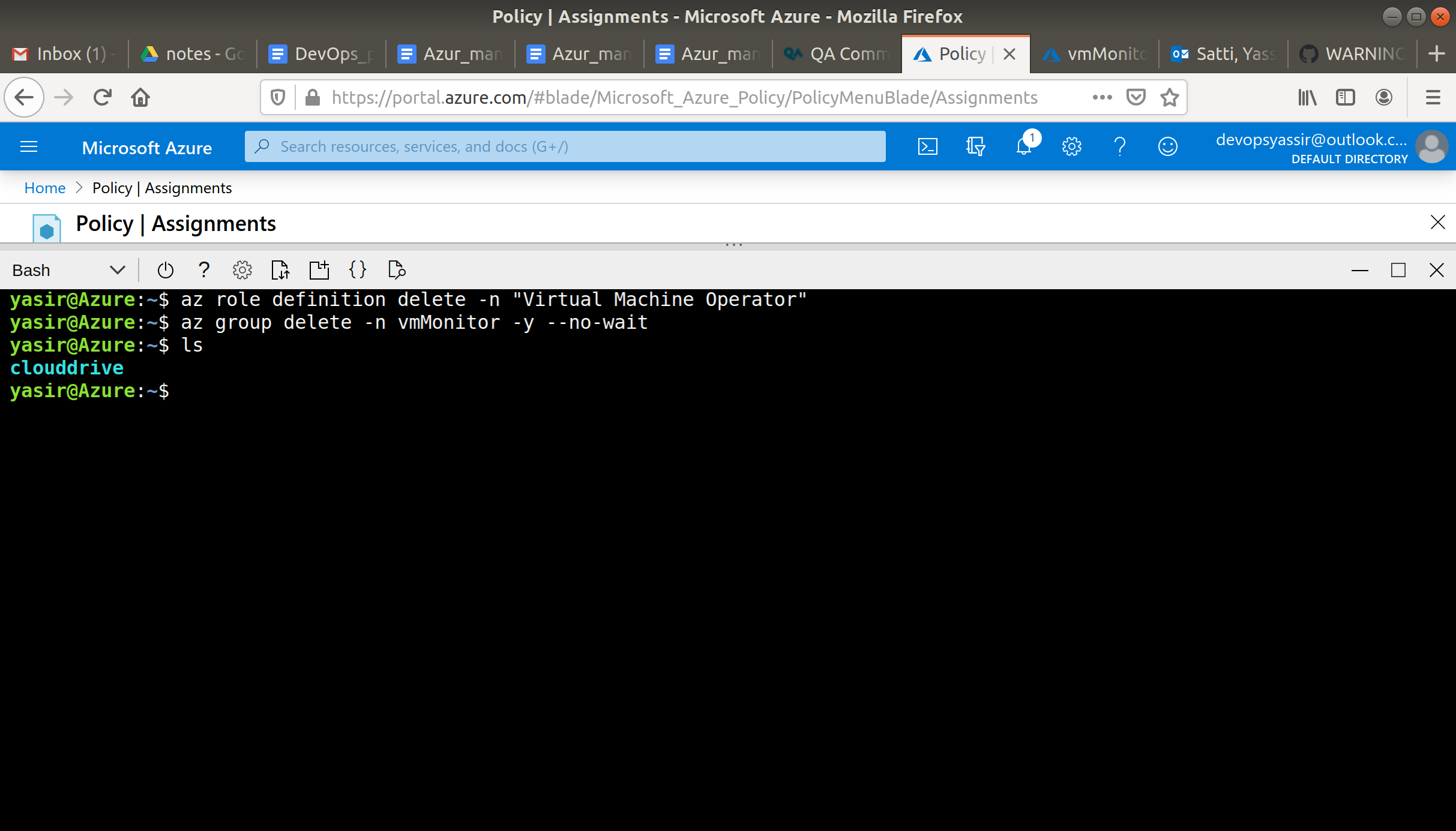
**The scope has successfully been changed to this resource group!**

1. Delete the role with:

**az role definition delete -n "Virtual Machine Operator"**

1. Delete the resource group:

**az group delete -n vmMonitor -y --no-wait**

****

1. Delete json file:

cd

rm vm-operator.json

