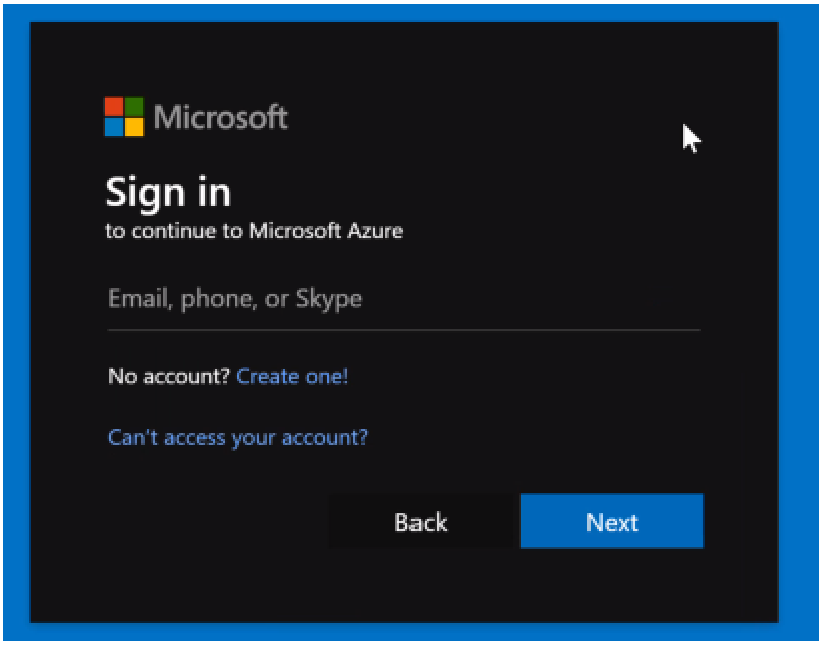
Create RBAC Custom Roles

Configure an Azure Cloud Shell Powershell Session

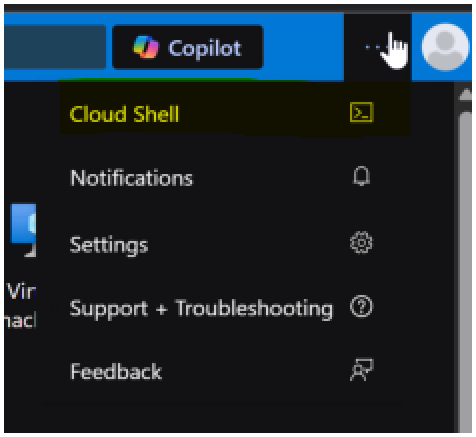
Log into the Admin Account



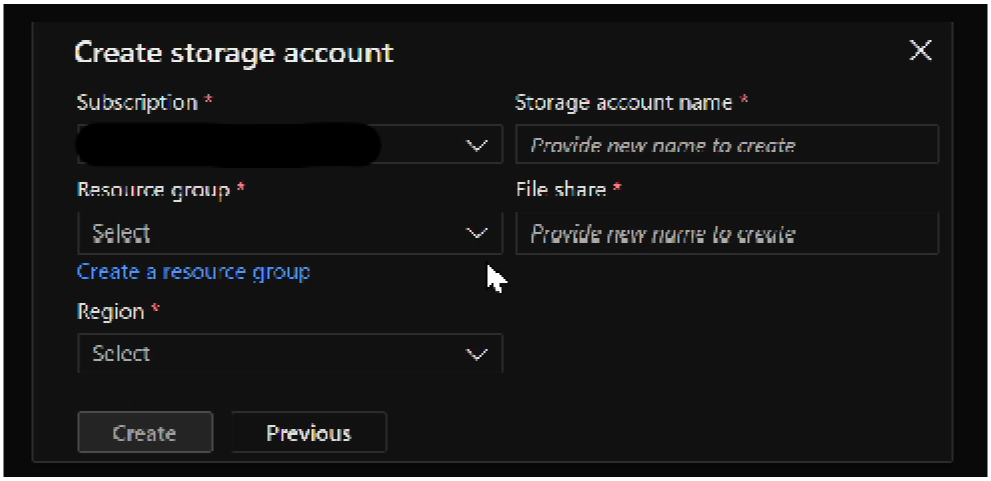
Sign in

to continue to Microsoft Azure

1. Open an Cloud Shell session



2. Select **PowerShell** once the Azure Cloud Shell dialog opens
3. Select **Mount Storage Account**, then choose your current subscription
4. Select **I want to create a storage account**, enter the necessary information, and select **Create** for deployment



Create storage account

Subscription *

[redacted]

Storage account name *

Provide new name to create

Resource group *

Select

File share *

Provide new name to create

Region *

Select

Deployment is in progress

If you are using Azure Cloud Shell for the first time, you will be prompted to configure a storage account. This storage account will log all pertinent information from the shell. Azure Cloud Shell requires both a storage account and a file share to store commands and scripts.

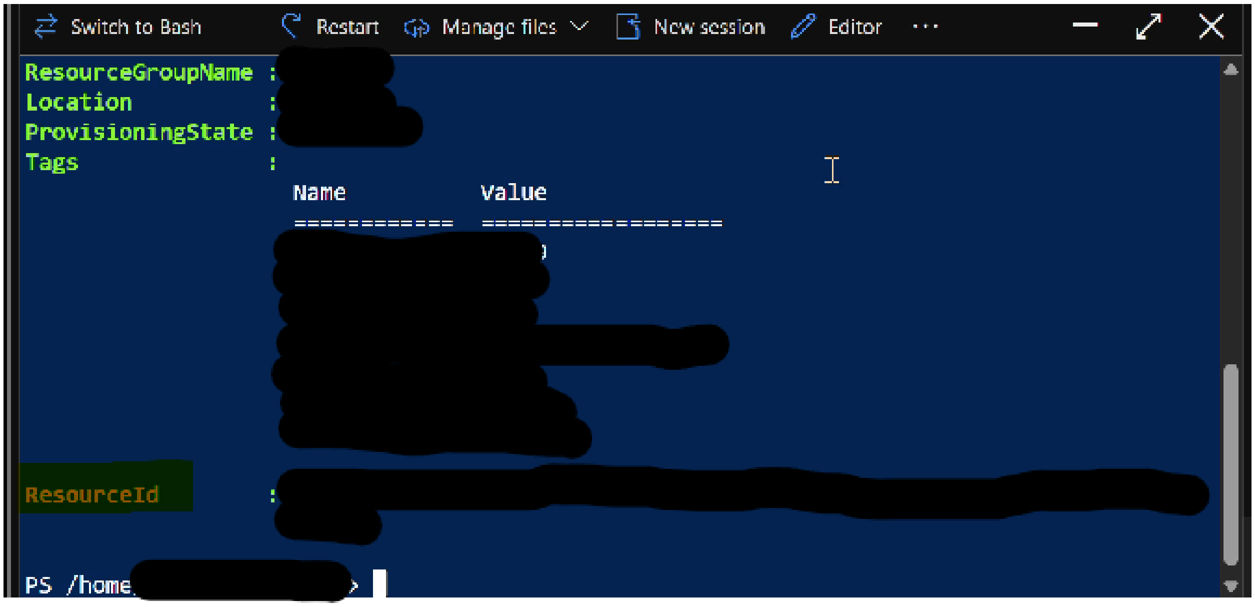
Note: Azure Cloud Shell can interpret both PowerShell and Bash.

Create a Custom Role Using Azure PowerShell

Retrieve the Resource ID of the Resource Group

Run the following command to obtain the resource ID:

Get-AzResourceGroup -Name {ResourceGroupName}



```
ResourceGroupName : [redacted]
Location          :
ProvisioningState :
Tags              :
                    Name          Value
                    ============  ==================
                    [redacted]

ResourceId        : [redacted]

PS /home[redacted]>
```

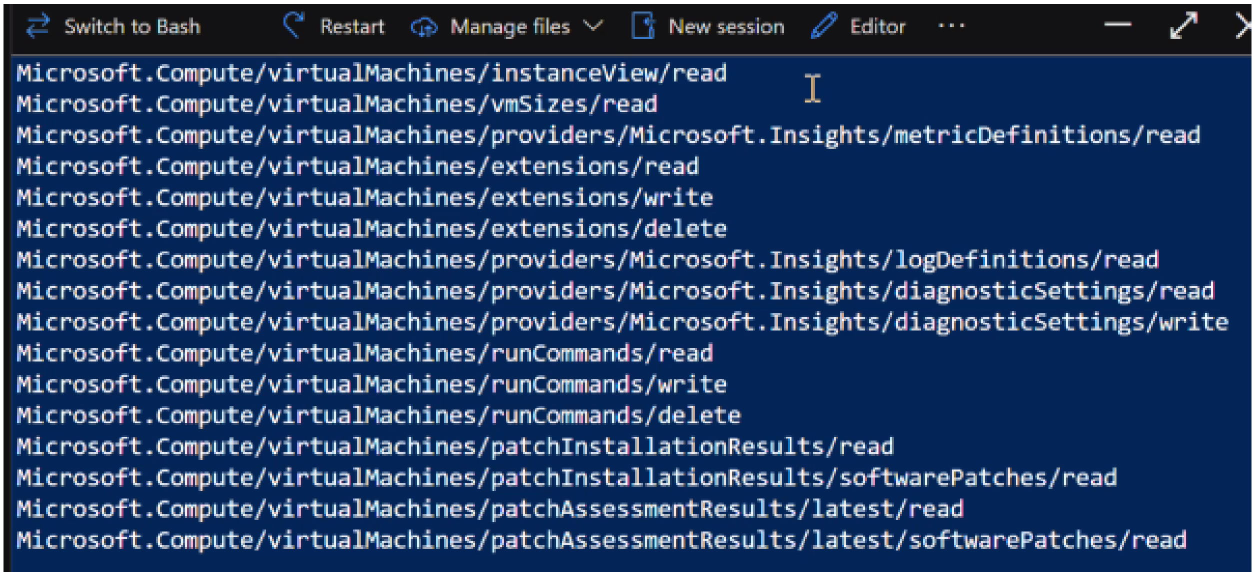
You should receive an output similar to the following. Pay close attention to the bottom where it says **ResourceId**.

Identify Operations Associated with Virtual Machines

Run the following command:

Get-AzProviderOperation "Microsoft.Compute/virtualmachines/" | FT Operation, Description -Auto*

This will output a list of operations related to virtual machines.

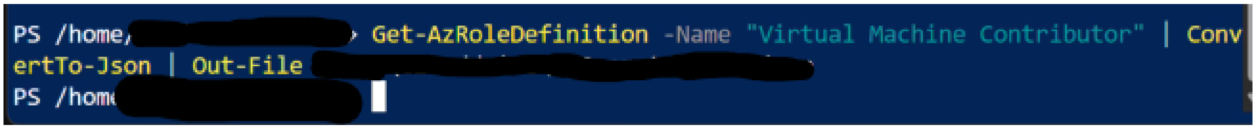


```
Microsoft.Compute/virtualMachines/instanceView/read
Microsoft.Compute/virtualMachines/vmSizes/read
Microsoft.Compute/virtualMachines/providers/Microsoft.Insights/metricDefinitions/read
Microsoft.Compute/virtualMachines/extensions/read
Microsoft.Compute/virtualMachines/extensions/write
Microsoft.Compute/virtualMachines/extensions/delete
Microsoft.Compute/virtualMachines/providers/Microsoft.Insights/logDefinitions/read
Microsoft.Compute/virtualMachines/providers/Microsoft.Insights/diagnosticSettings/read
Microsoft.Compute/virtualMachines/providers/Microsoft.Insights/diagnosticSettings/write
Microsoft.Compute/virtualMachines/runCommands/read
Microsoft.Compute/virtualMachines/runCommands/write
Microsoft.Compute/virtualMachines/runCommands/delete
Microsoft.Compute/virtualMachines/patchInstallationResults/read
Microsoft.Compute/virtualMachines/patchInstallationResults/softwarePatches/read
Microsoft.Compute/virtualMachines/patchAssessmentResults/latest/read
Microsoft.Compute/virtualMachines/patchAssessmentResults/latest/softwarePatches/read
```

Retrieve and Modify the Role Definition

Now, retrieve the role definition of the **Virtual Machine Contributor** role and output it to a JSON file:

Get-AzRoleDefinition -Name “Virtual Machine Contributor” | ConvertTo-Json | Out-File $home\clouddrive\VMOperatorRole.json



```
PS /home/[redacted]> Get-AzRoleDefinition -Name "Virtual Machine Contributor" | Conv
ertTo-Json | Out-File [redacted]
PS /hom[redacted]
```

Azure RBAC role assignments can grant access to resources at different scopes, such as subscriptions, resource groups, or specific resources, by assigning a role to a user or group. There are two types of roles: built-in and custom.

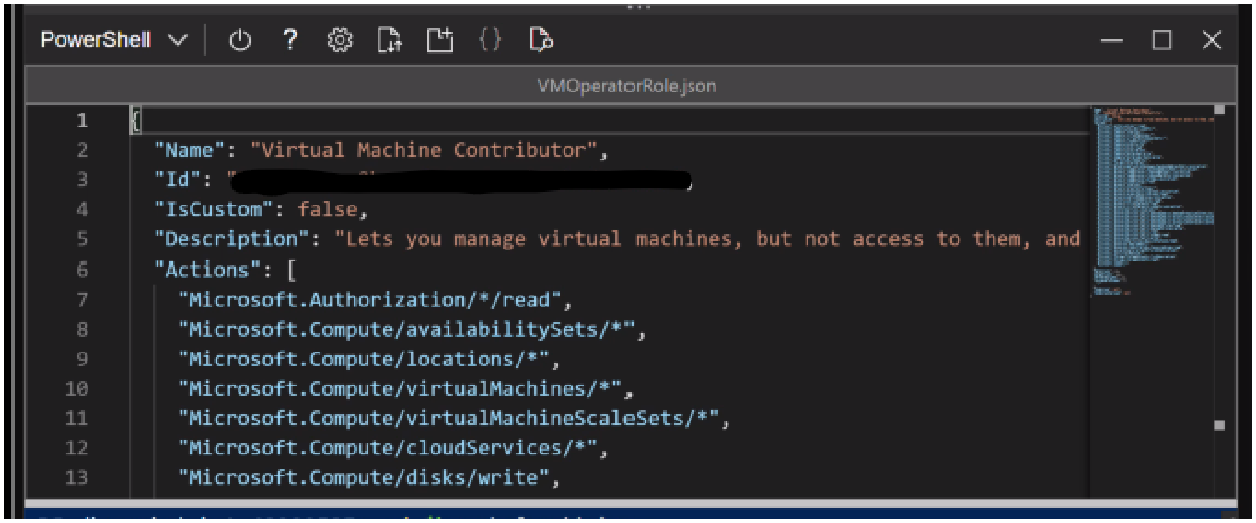
Open and Edit the JSON File

1. Navigate to the directory:

   cd $home\clouddrive

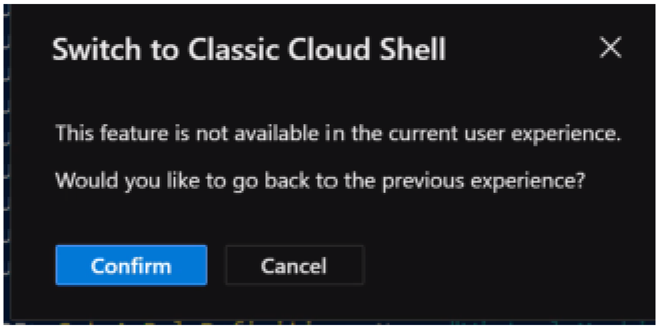
2. Open the JSON file in the shell code editor:

   code VMOperatorRole.json



```
{
  "Name": "Virtual Machine Contributor",
  "Id": "[redacted]
  "IsCustom": false,
  "Description": "Lets you manage virtual machines, but not access to them, and
  "Actions": [
    "Microsoft.Authorization/*/read",
    "Microsoft.Compute/availabilitySets/*",
    "Microsoft.Compute/locations/*",
    "Microsoft.Compute/virtualMachines/*",
    "Microsoft.Compute/virtualMachineScaleSets/*",
    "Microsoft.Compute/cloudServices/*",
    "Microsoft.Compute/disks/write",
```

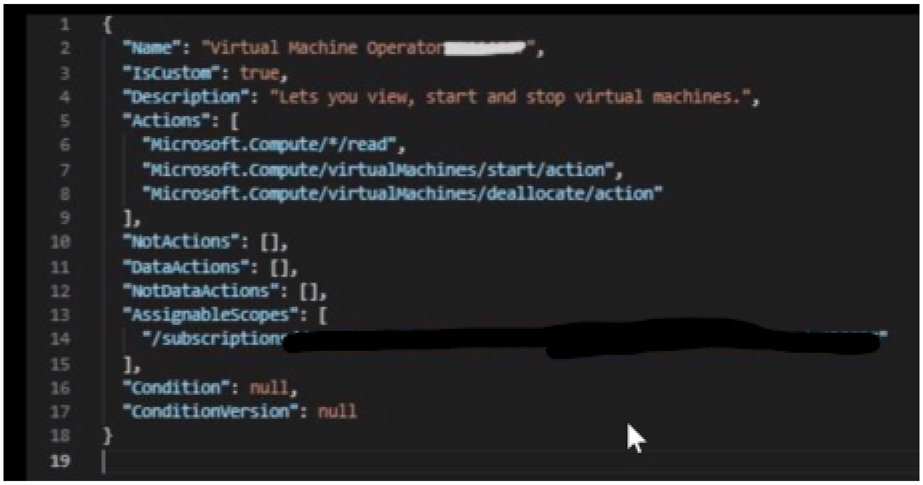
Note: If prompted to switch to Cloud Shell Classic, rerun the commands.


Switch to Classic Cloud Shell

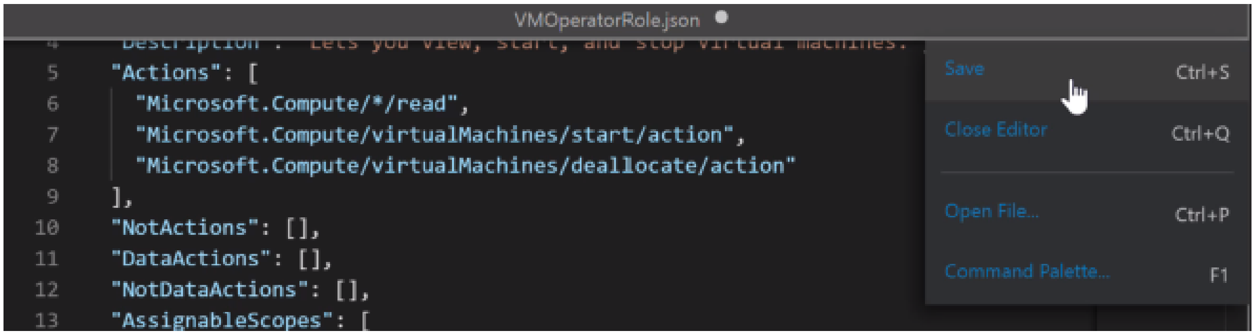
This feature is not available in the current user experience.

Would you like to go back to the previous experience?

3. Edit the JSON file, modifying only the following fields:
   - Name
   - IsCustom
   - Description
   - AssignableScopes
   - Actions
4. Save the file



```
{
  "Name": "Virtual Machine Operator[redacted]",
  "IsCustom": true,
  "Description": "Lets you view, start and stop virtual machines.",
  "Actions": [
    "Microsoft.Compute/*/read",
    "Microsoft.Compute/virtualMachines/start/action",
    "Microsoft.Compute/virtualMachines/deallocate/action"
  ],
  "NotActions": [],
  "DataActions": [],
  "NotDataActions": [],
  "AssignableScopes": [
    "/subscription[redacted]"
  ],
  "Condition": null,
  "ConditionVersion": null
}
```

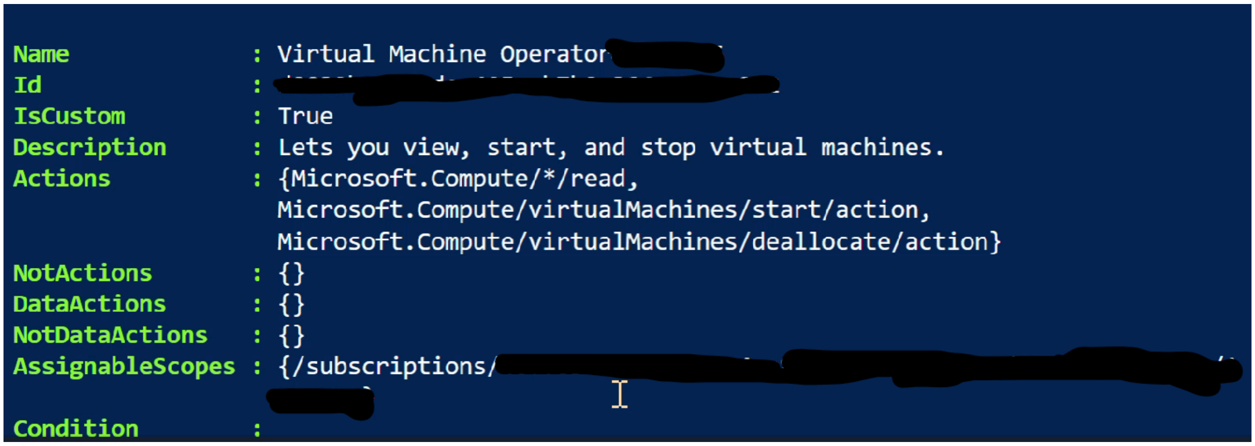


```
  "Description": "Lets you view, start, and stop virtual machines.
  "Actions": [
    "Microsoft.Compute/*/read",
    "Microsoft.Compute/virtualMachines/start/action",
    "Microsoft.Compute/virtualMachines/deallocate/action"
  ],
  "NotActions": [],
  "DataActions": [],
  "NotDataActions": [],
  "AssignableScopes": [
```

Create the Custom Role

After saving the file, create the new custom role by running:

New-AzRoleDefinition -InputFile “VMOperatorRole.json”



```
Name             : Virtual Machine Operator[redacted]
Id               : [redacted]
IsCustom         : True
Description      : Lets you view, start, and stop virtual machines.
Actions          : {Microsoft.Compute/*/read,
                   Microsoft.Compute/virtualMachines/start/action,
                   Microsoft.Compute/virtualMachines/deallocate/action}
NotActions       : {}
DataActions      : {}
NotDataActions   : {}
AssignableScopes : {/subscriptions/[redacted]

Condition        :
```

You have now successfully created a custom role using Azure PowerShell.

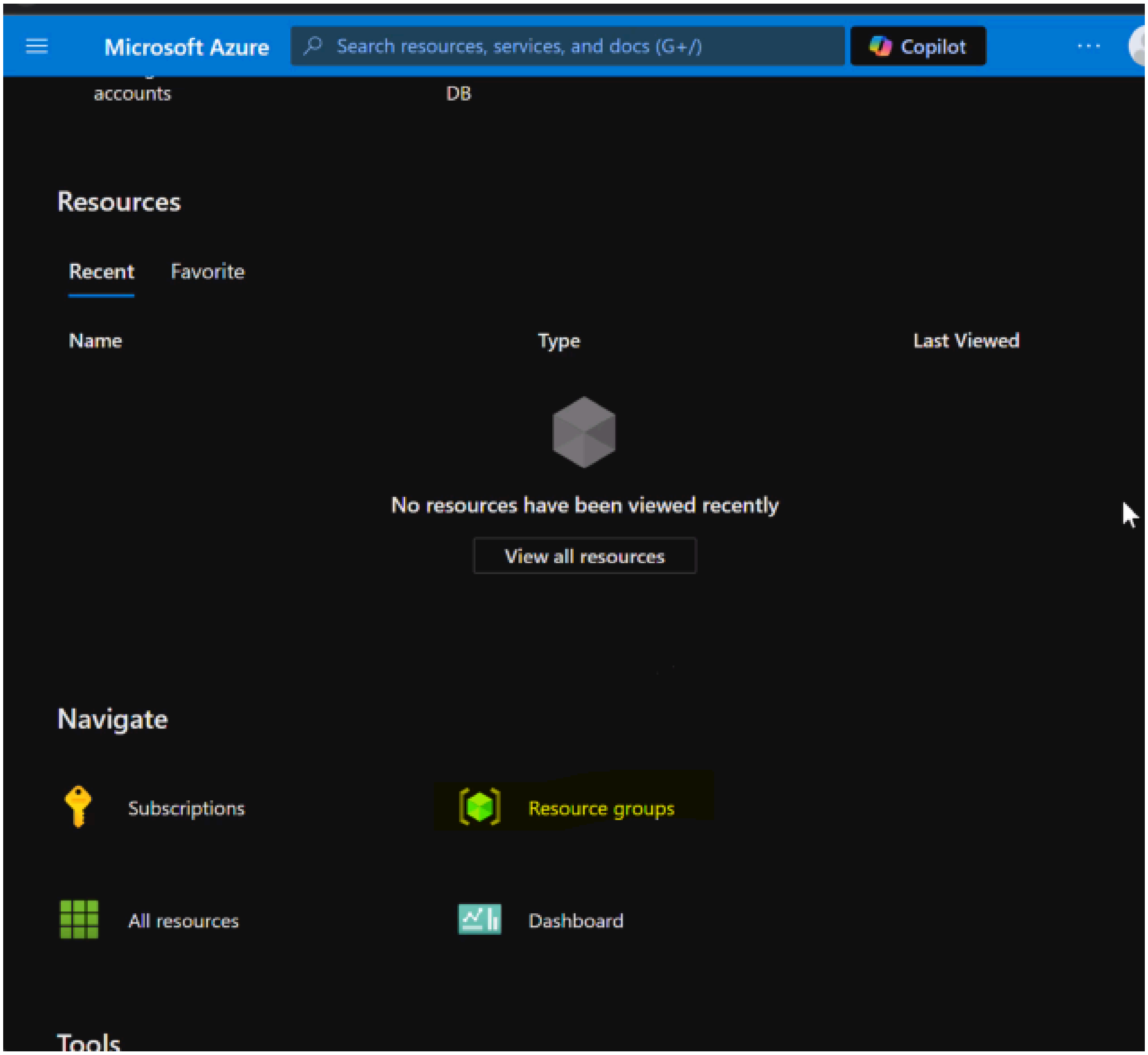
Create a Custom Role Using the Azure Portal

1. Close the Cloud Shell session
2. Retrieve the permissions granted to the **Storage Account Contributor** role in the Azure portal

What is a Storage Account Contributor? A Storage Account Contributor is a role that allows users to manage storage accounts but not access their data.

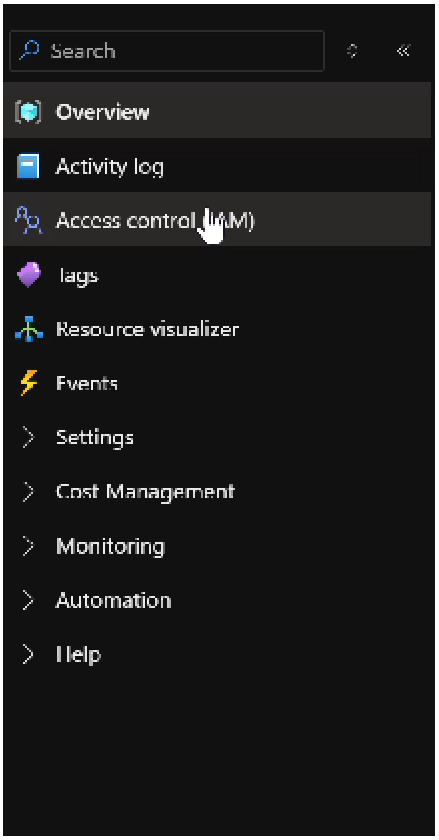
Continued Steps to Create a Custom Role in the Azure Portal

3. In the Azure portal, select **Resource Groups**

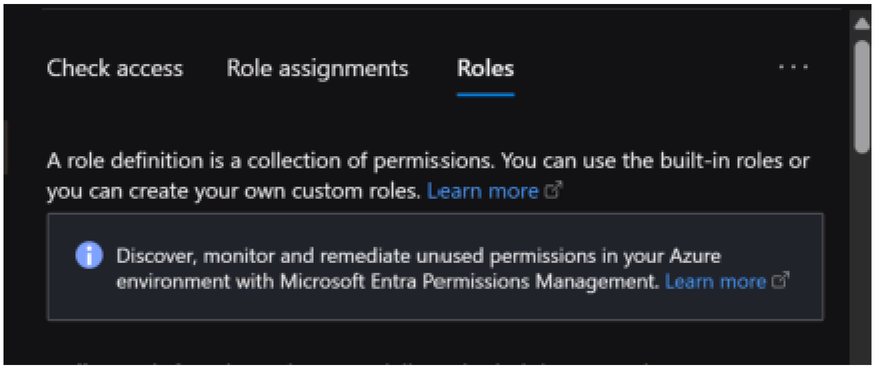


4. Select the desired resource group

5. In the **Service Menu**, select **Access Control (IAM)**



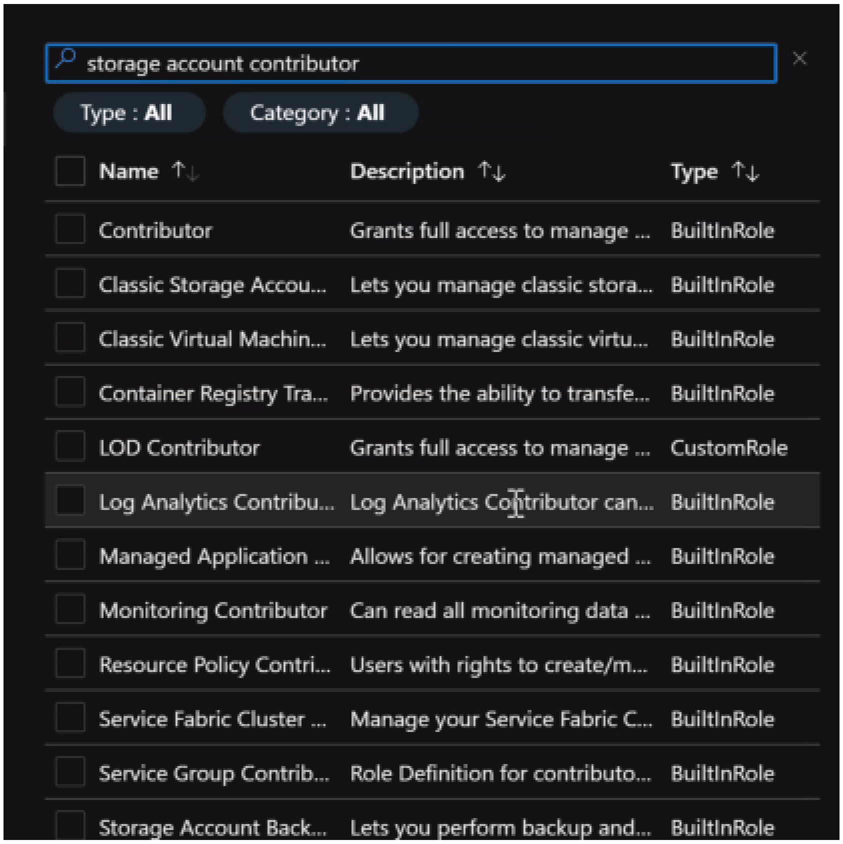
6. Navigate to the **Roles** tab



A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. Learn more

Discover, monitor and remediate unused permissions in your Azure environment with Microsoft Entra Permissions Management. Learn more

7. Enter *storage account contributor* in the search bar

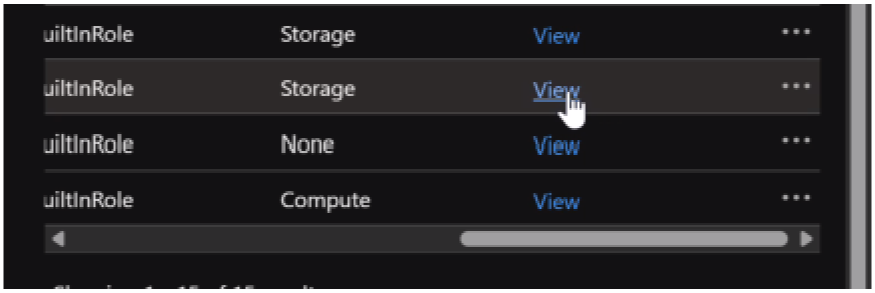


storage account contributor

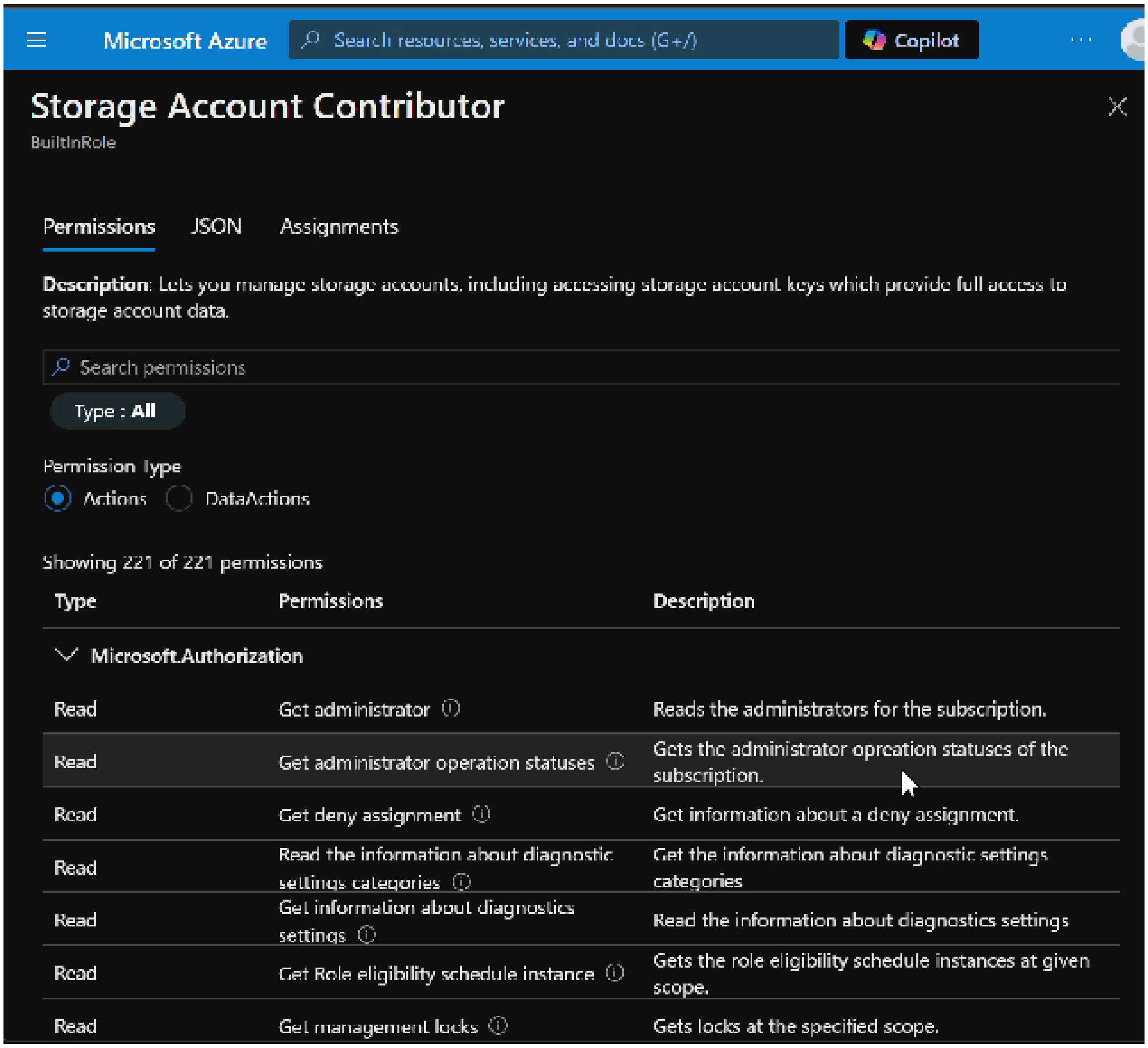
Type : All   Category : All

□	Name	Description	Type
□	Contributor	Grants full access to manage ...	BuiltInRole
□	Classic Storage Accou...	Lets you manage classic stora...	BuiltInRole
□	Classic Virtual Machin...	Lets you manage classic virtu...	BuiltInRole
□	Container Registry Tra...	Provides the ability to transfe...	BuiltInRole
□	LOD Contributor	Grants full access to manage ...	CustomRole
□	Log Analytics Contribu...	Log Analytics Contributor can...	BuiltInRole
□	Managed Application ...	Allows for creating managed ...	BuiltInRole
□	Monitoring Contributor	Can read all monitoring data ...	BuiltInRole
□	Resource Policy Contri...	Users with rights to create/m...	BuiltInRole
□	Service Fabric Cluster ...	Manage your Service Fabric C...	BuiltInRole
□	Service Group Contrib...	Role Definition for contributo...	BuiltInRole
□	Storage Account Back...	Lets you perform backup and...	BuiltInRole

8. Select **Storage Account Contributor**, then click **View** to review the permissions granted



uiltInRole	Storage	View	···
uiltInRole	Storage	View	···
uiltInRole	None	View	···
uiltInRole	Compute	View	···



Storage Account Contributor

BuiltInRole

Description: Lets you manage storage accounts, including accessing storage account keys which provide full access to storage account data.

Permission Type

● Actions ○ DataActions

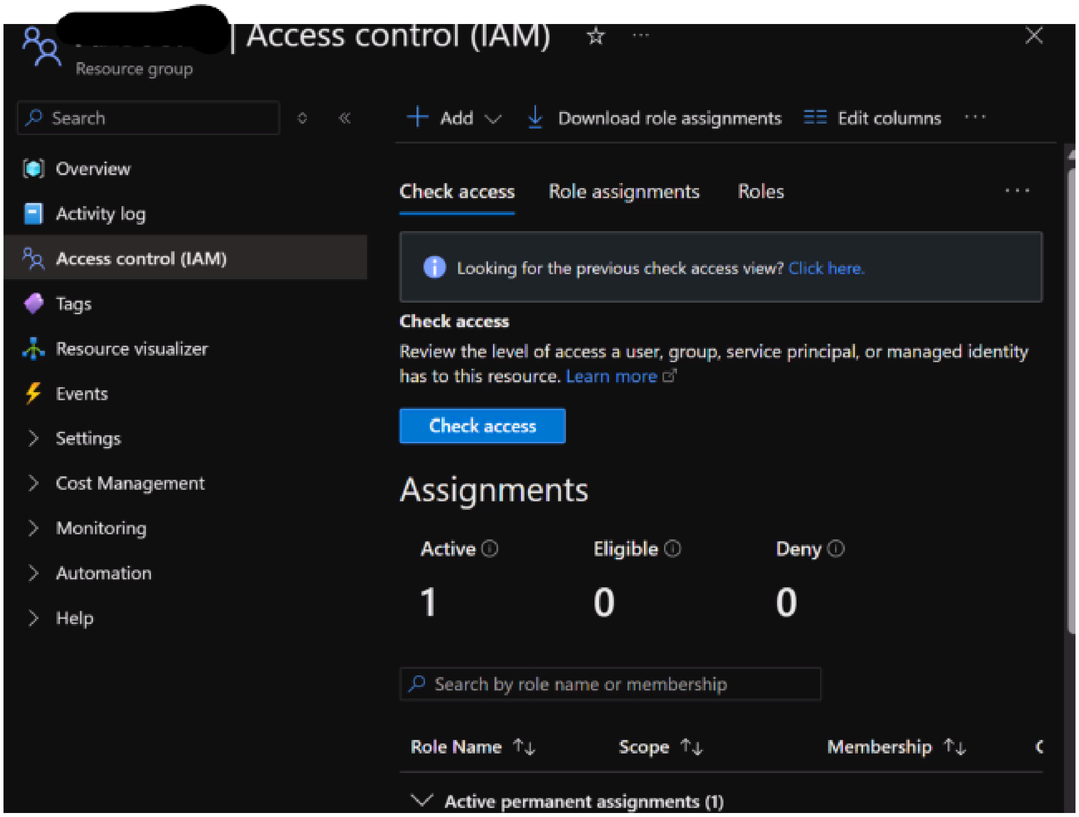
Showing 221 of 221 permissions

Type	Permissions	Description
Microsoft.Authorization		
Read	Get administrator ⓘ	Reads the administrators for the subscription.
Read	Get administrator operation statuses ⓘ	Gets the administrator operation statuses of the subscription.
Read	Get deny assignment ⓘ	Get information about a deny assignment.
Read	Read the information about diagnostic settings categories ⓘ	Get the information about diagnostic settings categories
Read	Get information about diagnostics settings ⓘ	Read the information about diagnostics settings
Read	Get Role eligibility schedule instance ⓘ	Gets the role eligibility schedule instances at given scope.
Read	Get management locks ⓘ	Gets locks at the specified scope.

Clone and Modify the Role

Now we will create a custom role that is based on the Storage Account Contributor role.

1. Return to the **Resource Group** page
2. Select the desired resource group
3. Navigate to **Access Control (IAM)**
4. Select **Check Access**



Looking for the previous check access view? Click here.

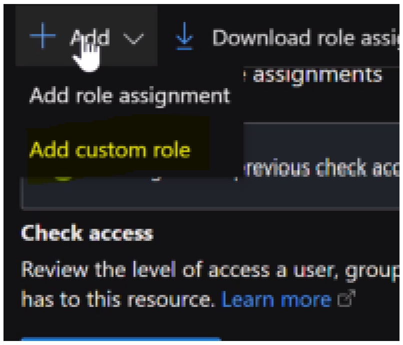
Check access

Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

Active	Eligible	Deny
1	0	0

Active permanent assignments (1)

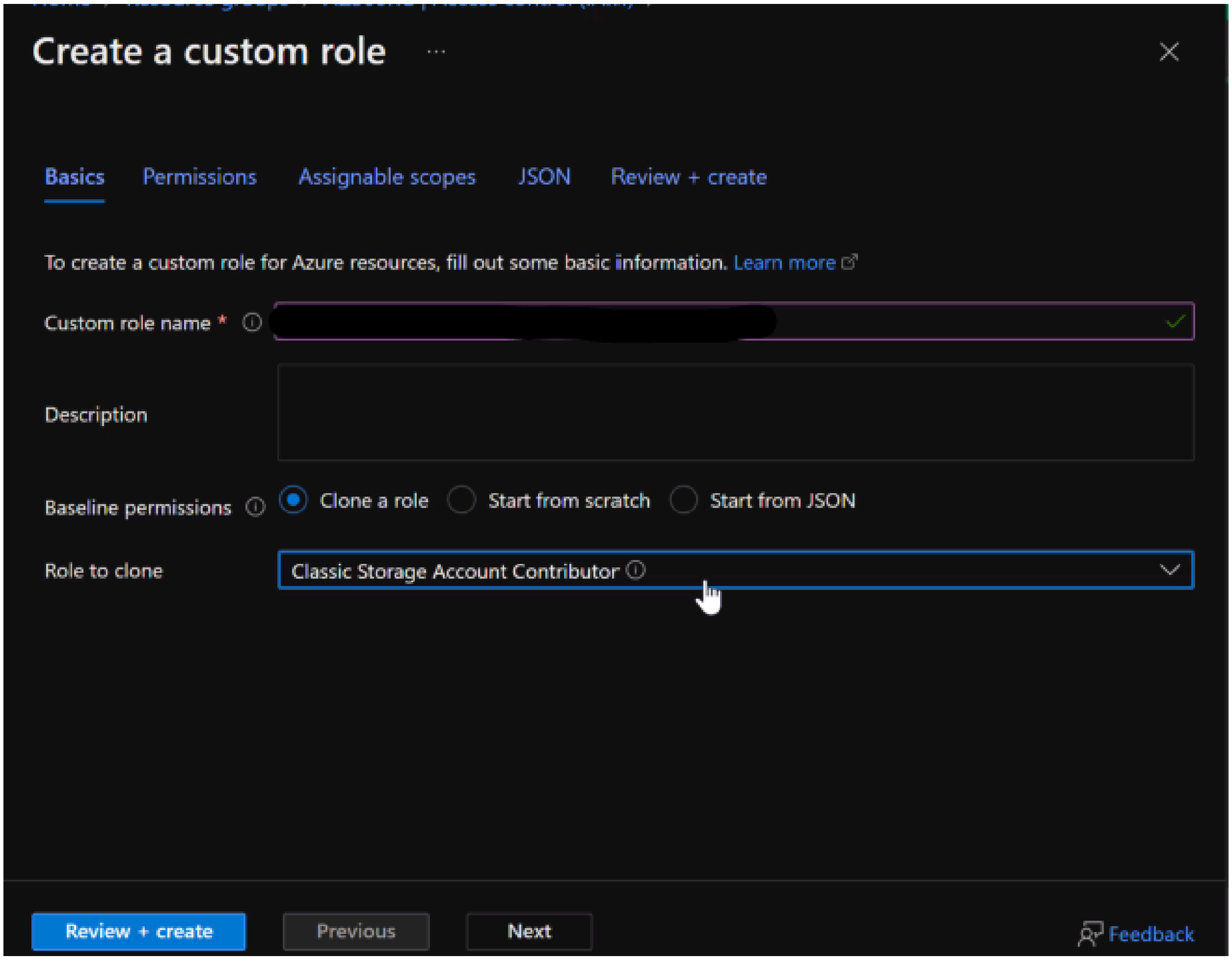
5. Select **Add**, then choose **Add Custom Role**



Check access

Review the level of access a user, group has to this resource. Learn more

6. Enter the custom role name
7. Select **Clone a Role** and choose **Storage Account Contributor**
8. Click **Next**



To create a custom role for Azure resources, fill out some basic information. Learn more

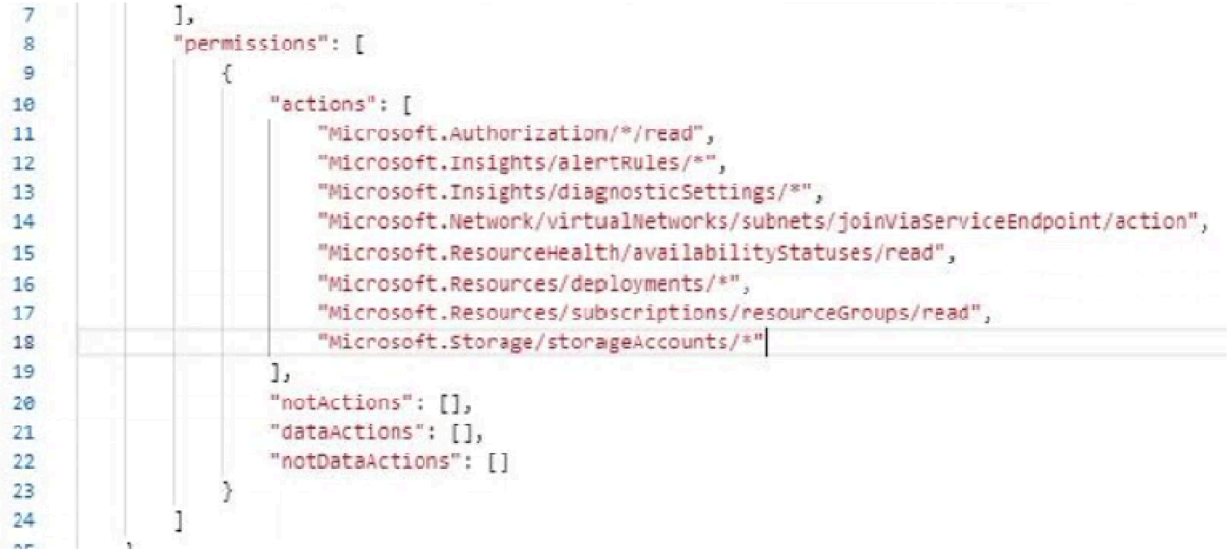
Custom role name * [redacted] ✓

Description

Baseline permissions ● Clone a role ○ Start from scratch ○ Start from JSON

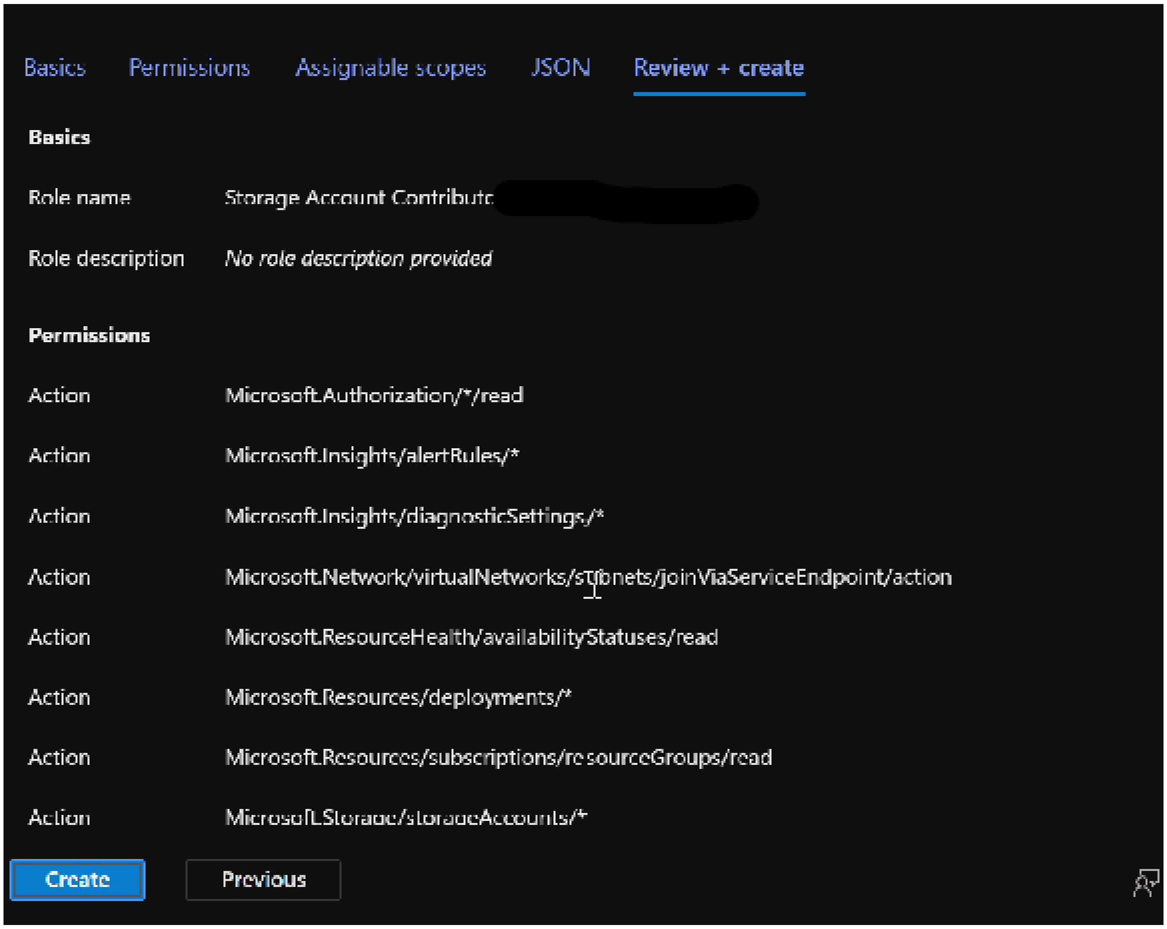
Role to clone: Classic Storage Account Contributor

9. On the **Permissions** page, review and click **Next**
10. Ensure the **Assignable Scope** is correct (it should be limited to the current resource group), then click **Next**
11. On the JSON page, select **Edit**
12. Modify the necessary **actions** to look like the following:



```
        ],
        "permissions": [
            {
                "actions": [
                    "Microsoft.Authorization/*/read",
                    "Microsoft.Insights/alertRules/*",
                    "Microsoft.Insights/diagnosticSettings/*",
                    "Microsoft.Network/virtualNetworks/subnets/joinViaServiceEndpoint/action",
                    "Microsoft.ResourceHealth/availabilityStatuses/read",
                    "Microsoft.Resources/deployments/*",
                    "Microsoft.Resources/subscriptions/resourceGroups/read",
                    "Microsoft.Storage/storageAccounts/*"
                ],
                "notActions": [],
                "dataActions": [],
                "notDataActions": []
            }
        ]
```

13. Click **Review + Create**, then **Create**



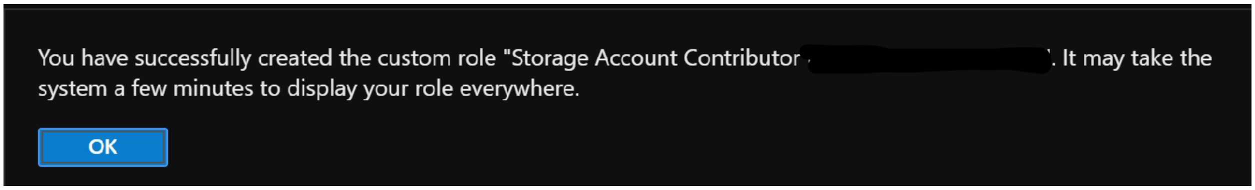
Basics

Role name Storage Account Contribut[redacted]

Role description *No role description provided*

Permissions

Action	Microsoft.Authorization/*/read
Action	Microsoft.Insights/alertRules/*
Action	Microsoft.Insights/diagnosticSettings/*
Action	Microsoft.Network/virtualNetworks/subnets/joinViaServiceEndpoint/action
Action	Microsoft.ResourceHealth/availabilityStatuses/read
Action	Microsoft.Resources/deployments/*
Action	Microsoft.Resources/subscriptions/resourceGroups/read
Action	Microsoft.Storage/storageAccounts/*



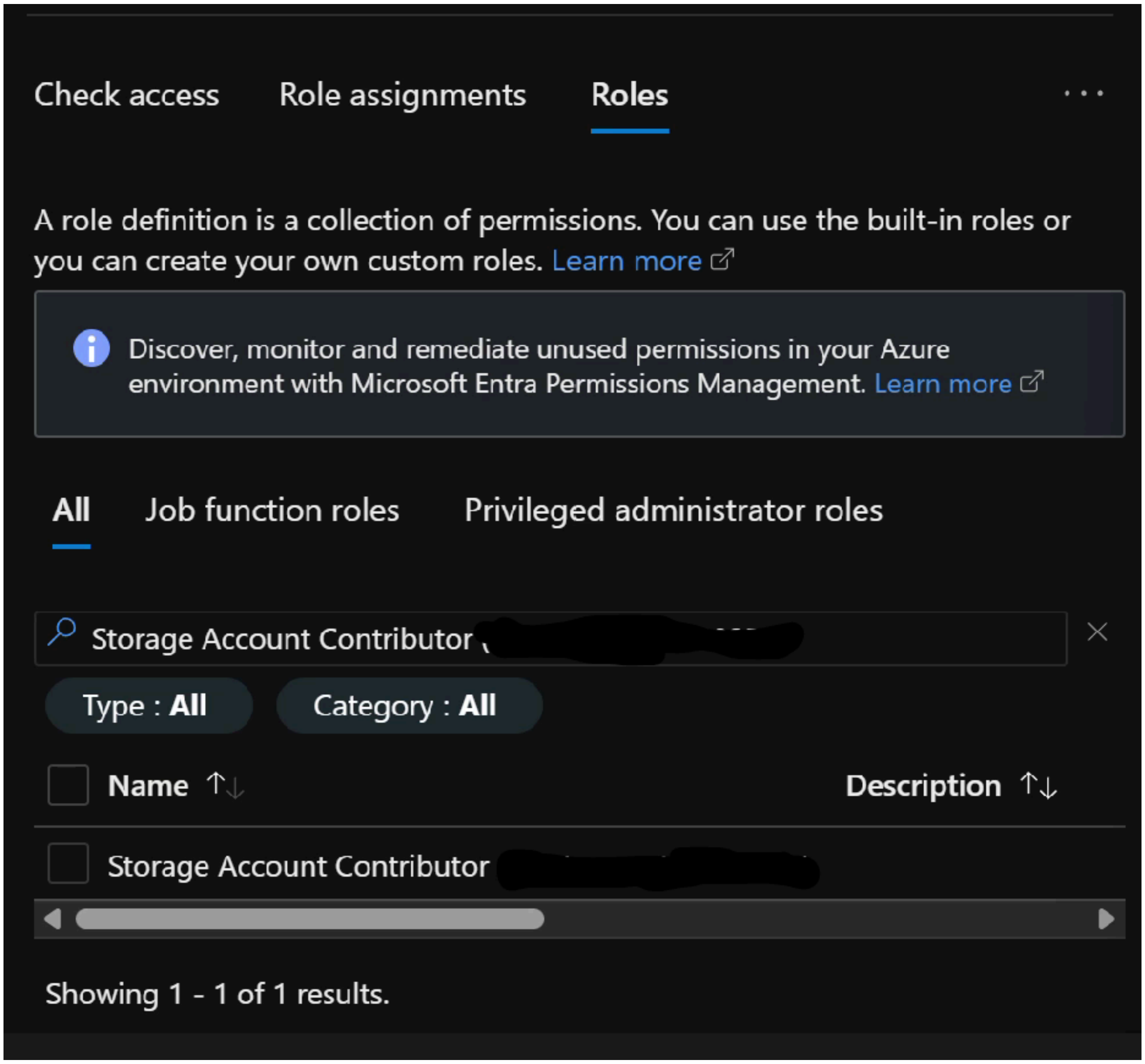
You have successfully created the custom role "Storage Account Contributor [redacted]". It may take the system a few minutes to display your role everywhere.

14. Select **OK**

Verify the Custom Role

Retrieve the **Storage Account Contributor** role and confirm that it does not contain the **Microsoft.Support** provider.

What is the Microsoft.Support provider? The **Microsoft.Support** provider is used for support-related access permissions in Azure.



A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. Learn more

Discover, monitor and remediate unused permissions in your Azure environment with Microsoft Entra Permissions Management. Learn more

Storage Account Contributor [redacted]

Type : **All** Category : **All**

□	Name ↑↓	Description ↑↓
□	Storage Account Contributor [redacted]	

Showing 1 - 1 of 1 results.

We have successfully:

- Configured an Azure Cloud Shell PowerShell session.
- Created a custom role using Azure PowerShell.
- Created a custom role using the Azure portal.

Your RBAC custom role is now fully configured and ready for use!