Create a Data Factory Pipeline Level custom role

Last updated by | Veena Pachauri | Jan 16, 2023 at 3:32 AM PST

Install Azure CLI:

https://docs.microsoft.com/en-us/cli/azure/install-azure-cli-windows?view=azure-cli-latest ☒

Open Powershell in Admin mode
Get the built-in permission and attribute it to a variable:

```
PS C:\> $role = Get-AzRoleDefinition -Name "Data Factory Contributor"
```

Check the role actions:

```
PS C:\> $role.Actions
Microsoft.Authorization/*/read
Microsoft.DataFactory/dataFactories/*
Microsoft.DataFactory/factories/*
Microsoft.Insights/alertRules/*
Microsoft.ResourceHealth/availabilityStatuses/read
Microsoft.Resources/deployments/*
Microsoft.Resources/subscriptions/resourceGroups/read
Microsoft.Support/*
```

Customer wants to have only run permissions for the new role. As per below link , createrun is the required permission:

Azure resource provider operations | Microsoft Docs ☒

Clear the existent Actions and include the new one

```
$role.Actions.Clear()
$role.Actions.Add("Microsoft.DataFactory/factories/pipelines/createrun/action")
```

Clear the existent assignable Scope and include the new one

```
$role.AssignableScopes.Clear()
$role.AssignableScopes.Add("/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/resourceGroups/<YourResourceGr
```

◀ ━━━━━━━━━━━━━━━━━━ ▶

Clear and change the properties below accordingly:

```
PS C:\> $role.Id = $null
PS C:\> $role.Name = "Data Factory Custom Pipeline Role"
PS C:\> $role.Description = "Data Factory Contributor with restricted permissions"
```

Finally create the role:

```
PS C:\> New-AzRoleDefinition -Role $role
```

output:

```
Name              : Data Factory Custom Pipeline Role
Id                : [NEW_ID]
IsCustom          : True
Description       : Data Factory Contributor with restricted permissions
Actions           : {Microsoft.DataFactory/factories/pipelines/createrun/action}
NotActions        : {}
DataActions       : {}
NotDataActions    : {}
AssignableScopes  : {/ subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/resourceGroups/<YourResourceGroupName
```

◄ ▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬   ▶

Points to Remember:

1. You won't be able to see this new custom role in Custom roles list as "assignableScopes" (pipeline scope in this use case) is not officially part of it. So, you won't be able to see it when you try to use this from Azure Portal "Access Control (IAM) -> Role assignments" . But you can use/assign this custom role to a user using Powershell.

2. To assign this custom role (only run a particular ADF pipeline) to a user, please use below command:

```
New-AzRoleAssignment -ObjectId "<ObjectID of the user>" -RoleDefinitionName "<Your Custom Role Name (In this e
```

◄ ▬▬▬▬▬▬▬▬▬▬▬   ▶

3. Assign "Reader" built in at Resource (ADF) level for the user.

4. Assign Custom Role (only to run a particular pipeline - "Run Data Factory pipeline" in this example) at Resource (ADF) level for the user.

5. All changes to pipeline level role should be done through CLI . JSON changes through portal cause inconsistent behaviour .

Additional Information:

- **Icm References:**
- **Author:** swbabber
- **Reviewer:** grorcai
- **Keywords:** Pipeline Level custom role

How good have you found this content?