Azure RBAC permissions

Last updated by | Lisa Liu | Nov 6, 2020 at 10:35 AM PST

Azure RBAC permissions

Tuesday, August 29, 2017
4:49 PM

A Customer may want to give another user permissions to create a PostgreSQL (or MySQL) server but found only contributor works and will give way more access than they want. Currently have to build a custom one. Hopefully a role will be added in the future.

The different permissions needed are below to give all access to Postgres, you could refine this to only servers for instance with Microsoft.DBforPostgreSQL/Servers/* or to only read with M This is not specific to Postgres and can be done for MySQL as well by using the DBforMySQL namespace.

```
Microsoft.Resources/Deployments/Write

Microsoft.DBforPostgreSQL/*
```

To actually create the role we are going to use powershell. https://docs.microsoft.com/en-us/powershell/module/azurerm.resources/new-azurermroledefinition?view=azurermps-4.3.1

```
$role = Get-AzureRmRoleDefinition -Name "Contributor" #Get existing role for a template

$role.Id = $null #Clear the ID

$role.Name = "PostgreSQL Contributor" #Name the role

$role.Description = "Can manage all aspects of Azure DB for Postgres" #Give the role a description

$role.Actions.Remove("*") #Remove existing actions

$role.Actions.Add("Microsoft.Resources/Deployments/Write") #Assign deployment role, needed for deploying to Azure Resource groups

$role.Actions.Add("Microsoft.DBforPostgreSQL/*") #Assign all permissions on the DBforPostgreSQL namespace to allow, creating, reading and

$role.AssignableScopes.Clear() #Clear existing scope

$role.AssignableScopes.Add("/subscriptions/SUSBCRIPTION ID") #Add scope of role to specific subscription

New-AzureRmRoleDefinition -Role $role #Create role
```

Here is the results of a created role

```
Name             : PostgreSQL Contributor

Id               : 7dbb5301-235b-4f03-8715-8bea64054b75

IsCustom         : True

Description      : Can manage all aspects of Azure DB for Postgres

Actions          : {Microsoft.Resources/Deployments/Write, Microsoft.DBforPostgreSQL/*}

NotActions       : {Microsoft.Authorization/*/Delete, Microsoft.Authorization/*/Write, Microsoft.Authorization/elevateAccess/Action}

AssignableScopes : {/subscriptions/SUSBCRIPTION ID}
```

Now we can assign it to a user

```
New-AzureRmRoleAssignment -ResourceGroupName "RESOURCE GROUP" -SignInName "USER@NAME.COM" -RoleDefinitionName "PostgreSQL Contributor"
```

If you wanted to view the assignments you can use Get-AzureRmRoleAssignment

```
Get-AzureRmRoleAssignment -RoleDefinitionName "PostgreSQL Contributor"


RoleAssignmentId   : /subscriptions/e9e5fe1b-1208-4cf2-8708-f0610f0c383d/resourceGroups/nilop-sc-rg/providers/Microsoft.Authorization/rol
939d-ae65aee6c1b5

Scope              : /subscriptions/e9e5fe1b-1208-4cf2-8708-f0610f0c383d/resourceGroups/nilop-sc-rg

DisplayName        : My User

SignInName         : user@name.com

RoleDefinitionName : PostgreSQL Contributor

RoleDefinitionId   : 7dbb5301-235b-4f03-8715-8bea64054b75
```

```
ObjectId            : c179c854-10dc-4a9d-a55d-0d2c4d41b6ba

ObjectType          : User
```

Created with Microsoft OneNote 2016.

How good have you found this content?