Permission - RBAC, least privilege

Last updated by | Keith Elmore | Apr 5, 2021 at 7:57 AM PDT

Contents

- Issue
- Cause
- Resolution
- Classification

Issue

```
(…)does not have authorization to perform action 'Microsoft.Sql/locations/syncGroupOperationResults/read' over
```

Cause

Issue is that we need some permission at subscription level like:

```
"Microsoft.Sql/locations/syncMemberOperationResults/read"
"Microsoft.Sql/locations/syncAgentOperationResults/read"
"Microsoft.Sql/locations/syncGroupOperationResults/read"
```

Resolution

We ran some tests in order to set the least privilege. We created two custom roles, one with wider permissions that are set at Resource Group level and another role with some read permissions needed at the Subscription level.

For resource level we can have:

```
"Microsoft.Sql/servers/databases/syncGroups/read"
"Microsoft.Sql/servers/databases/syncGroups/write"
"Microsoft.Sql/servers/databases/syncGroups/triggerSync/action"
"Microsoft.Sql/servers/databases/syncGroups/cancelSync/action"
"Microsoft.Sql/servers/databases/syncGroups/refreshHubSchema/action"
"Microsoft.Sql/servers/databases/syncGroups/refreshHubSchemaOperationResults/read"
"Microsoft.Sql/servers/databases/syncGroups/syncMembers/read"
"Microsoft.Sql/servers/databases/syncGroups/syncMembers/write"
"Microsoft.Sql/servers/databases/syncGroups/syncMembers/refreshSchema/action"
"Microsoft.Sql/servers/databases/syncGroups/syncMembers/refreshSchemaOperationResults/read"
"Microsoft.Sql/servers/databases/syncGroups/syncMembers/schemas/read"
"Microsoft.Sql/servers/databases/syncGroups/logs/read"
"Microsoft.Sql/servers/databases/syncGroups/hubSchemas/read"
"Microsoft.Sql/locations/syncMemberOperationResults/read"
"Microsoft.Sql/locations/syncAgentOperationResults/read"
"Microsoft.Sql/locations/syncGroupOperationResults/read"
"Microsoft.Sql/locations/syncDatabaseIds/read"
"Microsoft.Sql/servers/databases/write")
"Microsoft.Sql/servers/databases/read")
"Microsoft.Sql/servers/syncAgents/read")
"Microsoft.Sql/servers/syncAgents/write")
"Microsoft.Sql/servers/syncAgents/generateKey/action")
"Microsoft.Sql/servers/syncAgents/linkedDatabases/read")
```

For subscription level we can have:

```
"Microsoft.Sql/locations/syncMemberOperationResults/read"
"Microsoft.Sql/locations/syncAgentOperationResults/read"
"Microsoft.Sql/locations/syncGroupOperationResults/read"
```

We can create a custom role with just this permissions using PowerShell and assign the role to the user in the subscription:

```
$role = Get-AzureRmRoleDefinition "SQL DB Contributor"
$role.Id = $null
$role.Name = "Data Sync Sub level"
$role.Description = "Data Sync Sub level"
$role.Actions.Clear()
$role.Actions.Add("Microsoft.Sql/locations/syncMemberOperationResults/read")
$role.Actions.Add("Microsoft.Sql/locations/syncAgentOperationResults/read")
$role.Actions.Add("Microsoft.Sql/locations/syncGroupOperationResults/read")
$role.AssignableScopes.Clear()
$role.AssignableScopes.Add("/subscriptions/Input SubscriptionId here")
$role.NotActions.Clear()
New-AzureRmRoleDefinition -Role $role
New-AzureRmRoleAssignment -RoleDefinitionName "Data Sync Sub level" -ServicePrincipalName xxxxxxxx-ab2c-44dd-a
```

Classification

Root cause Tree - DataSync/User issue/error/SetupSyncFail

How good have you found this content?

🙂 🙁