Lab 02a - Manage Subscriptions and RBAC

Objectives

In this lab, we will:

## Task 1: Implement Management Groups

## Task 2: Create custom RBAC roles

## Task 3: Assign RBAC roles

## Task 1: Implement Management Groups

In this task, we will create and configure management groups.

For us to create management groups we need to the Management groups blade. We need to review messages at the top of the Management groups blade. If we are seeing the message stating **You are registered as a directory admin but do not have the necessary permissions to access the root management group**, than we need to perform the following sequence of steps:

1. In the Azure portal, search for and select Azure Active Directory.
2. On the blade displaying properties of your Azure Active Directory tenant, in the vertical menu on the left side, in the Manage section, select Properties.
3. On the Properties blade of your Azure Active Directory tenant, in the Access management for Azure resources section, select Yes and then select Save.
4. Navigate back to the Management groups blade and select Refresh.

After we complete this steps, we can continue with creating management groups.

On the Management groups blade, we click + Create, and we create the group with the following settings:

| Setting | Value |
| --- | --- |
| Management group ID | **az104-02-mg1** |
| Management group display name | **az104-02-mg1** |

After everything is done, we get the following:

Management groups 
Default Directory 
Search 
Overview 
Get started 
Settings 
O 
CD 
Add subscription 
Refresh 
Expand / Collapse all 
Use management groups to group subscriptions. Click on an exisiting to drill in, view details 
and govern resources. Right-click on any subscription or management group to launch quick 
actions. Click the •Get Started" tab to leam more 
P Search by name or ID 
Showing I subscriptions in 2 groups 
Name 
Tenant Root Group 
Azure Pass - Sponsors... 
x 
x 
Total 
3e612f7 c-4e11-4f7f-baa8480bead007da 
u 104-02 -mg I 
9947c7d8-0002-4f95-9be2-e61cef4a15b3 

## Task 2: Create custom RBAC roles

In this task, we will create a definition of a custom RBAC role.

First we need to open the **az104-02a-customRoleDefinition.json** file and change the SUBSCRIPTION\_ID with our ID - **9947c7d8-0002-4f95-9be2-e61cef4a15b3.** When we save the changes to the file we need to upload it into the Cloud Shell home directory. After we upload the file, we will run the following in the Power Shell pane:

* New-AzRoleDefinition -InputFile $HOME/az104-02a-customRoleDefinition.json

PS /home/ana> 
Name 
IsCustom 
Description 
Actions 
NotActions 
DataActions 
New-AzR01eDefinition -InputFi1e $HOME/az1ø4-e2a-customRoleDefinition .json 
Support Request Contributor (Custom) 
• f47ee3b6-b85f-493ø-be1b-c21d13bbc7ec 
: True 
Allows to create support requests 
{Mic rosoft. Resources/ subscriptions/ resourceGroups/ read , 
Microsoft. Support/*} 
NotDataActions 
AssignableScopes : 
{ / providers /Microsoft . Management mgl, 
/subscriptions/9947c7d8-eeø2-4f95-9be2-e61cef4a15b3} 

## Task 3: Task 3: Assign RBAC roles

In this task, we will create an Azure Active Directory user, assign the RBAC role you created in the previous task to that user, and verify that the user can perform the task specified in the RBAC role definition.

We will add New user in the Azure Active Directory. We create the user with the following settings:

| Setting | Value |
| --- | --- |
| User name | **az104-02-aaduser1** |
| Name | **az104-02-aaduser1** |
| Let me create the password | enabled |
| Initial password | **Provide a secure password** |

After we create the new user we navigate back to the az104-02-mg1 management group and display its details. From there we click Access Control (IAM), click + Add and then Add role assignment. On the Role tab, we search for Support Request Contributor (Custom). There we select the Role and click Next. On the Members tab, we click + Select members and select user account **az104-02-aaduser1@nikolovskaana1outlook.onmicrosoft.com**. We Click Next and then Review and assign.

Next, we open InPrivate browser window, and we sign in to Azure portal using [**az104-02-aaduser1@nikolovskaana1outlook.onmicrosoft.com**](mailto:az104-02-aaduser1@nikolovskaana1outlook.onmicrosoft.com)**.** There we verify that this user can see all resource groups, but cannot see any resources.

All resources 
Default Directory (nikolovskaanaloutlook.onmicrosoft.com) 
+ Create Manage view v 
Refresh Export to CSV Open query 
Assign tags Delete 
x 
v More (l) 
Filter for any field... 
Unsecure resources 
List view 
Name TJ 
Subscription equals all 
Recommendations 
Resource group equals all X 
Type equals all X +7 Add filter 
No grouping 
Type t' 
Resource group 
Location 
Subscription 
No resources match your filters 
Try changing or clearing your filters. 
Create resources 
Learn more 
Clear filters 

Home > 
Resource groups 
Default Directory (nikolovskaanaloutlook.onmicrosoft.com) 
+ Create Manage view v 
Refresh Export to CSV Open query 
Assign tags 
Filter for any field... 
O Unsecure resources 
List view 
Name TJ 
Subscription equals all 
O Recommendations 
(o) cloud-shell-storageAvesteurope 
NetworkWatcherRG 
Location equals all X Add filter 
Subscription 
Azure Pass - Sponsorship 
Azure Pass - Sponsorship 
NO grouping 
Location 
West Europe 
west US 

After this we **Create a support request,** in the Help + support. We do this still in the InPrivate window. Next, on the Problem Description/Summary tab of the Help + support - New support request blade, type Service and subscription limits in the Summary field and select the Service and subscription limits (quotas) issue type. Note that the subscription we are using in this lab is listed in the Subscription drop-down list.

New support request 
1. Problem description 
2. Recommended solution 
Tell us your issue, and we'll help you resolve it. 
3, Additional details 
4 _ Review create 
Provide information about your billing, subscription, quota management. or technical issue (including requests for technical 
advice). 
Issue type 
Subscription * 
Quota type * 
Service and subscription limits (quotas) 
Azure Pass - sponsorship (9947c7d8-0002-4f95-9be2-e61cef4a15b3) 
Can't find your subscription? Show more@ 
Select a quota type 

Here we do not continue with creating the support request. Instead, we sign out and close the InPrivate window we were using.