

Lab requirements

This lab requires permissions to create Azure Active Directory (Azure AD) users, create custom Azure Role Based Access Control (RBAC) roles, and assign these roles to Azure AD users.

Task 1: Implement Management Groups

On the **Management groups** blade, click **+ Create**.

The screenshot shows the Azure portal interface for a management group named 'az104-02-mg1'. The left sidebar contains navigation links for Overview, Subscriptions, Resource Groups, Resources, Activity Log, Access control (IAM), Governance, Get started, Security, Policy, Deployments, and Cost Management. The main content area displays the 'Essentials' section for the management group, including its Name, ID, Access Level (Owner), and Path. Below this, a table lists the subscriptions associated with the group. The table has columns for Name, ID, and Total subscriptions. One subscription is listed: 'az104-02-mg1' with ID 'az104-02-mg1' and 1 total subscription. Below the table, there is a link to 'Azure Pass - Sponsorship'.

Name	ID	Total subscriptions
az104-02-mg1	az104-02-mg1	1

Task 2: Create custom RBAC roles

Replace the `SUBSCRIPTION_ID` placeholder in the JSON file with the subscription ID and run the following to create the custom role definition: `New-AzRoleDefinition -InputFile $HOME/az104-02a-customRoleDefinition.json`

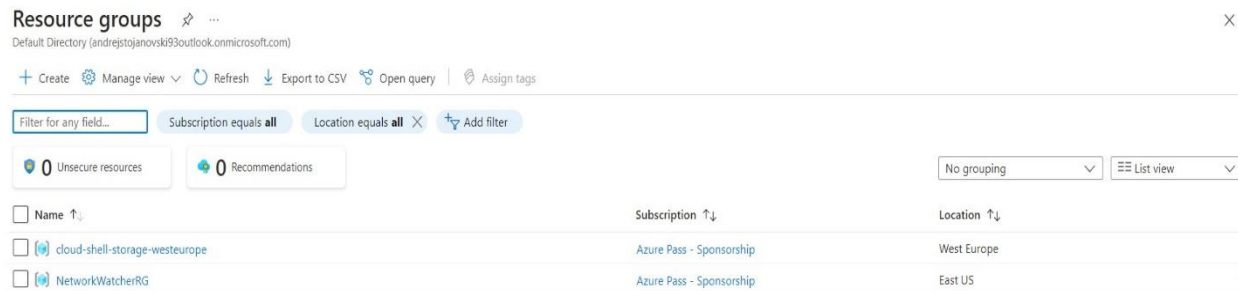
```
PS /home/andrej> ls -l
total 8
-rw-r--r-- 1 andrej andrej 433 Mar 26 11:36 az104-02a-customRoleDefinition.json
lrwxrwxrwx 1 andrej andrej 22 Mar 26 11:36 clouddrive -> /usr/csuser/clouddrive
drwxr-xr-x 3 andrej andrej 4096 Mar 26 08:05 Microsoft
PS /home/andrej> New-AzRoleDefinition -InputFile $HOME/az104-02a-customRoleDefinition.json

Name       : Support Request Contributor (Custom)
Id         : ccae05e-8040-47c4-8957-9e331c7cd8a3
IsCustom   : True
Description : Allows to create support requests
Actions    : (Microsoft.Resources/subscriptions/resourceGroups/read, Microsoft.Support/*)
NotActions : {}
DataActions : {}
NotDataActions : {}
AssignableScopes : (/providers/Microsoft.Management/managementGroups/az104-02-mg1, /subscriptions/6e58e49b-f4f5-4019-9ff0-b815383a0405)
```

Task 3: Assign RBAC roles

In the Azure portal, search for and select **Azure Active Directory**, on the Azure Active Directory blade, click **Users**, and then click + **New user**

1. In the **InPrivate** browser window, in the Azure portal, search and select **Resource groups** to verify that the az104-02-aaduser1 user can see all resource groups.



Resource groups

Default Directory (andrejstojanovski93outlook.onmicrosoft.com)

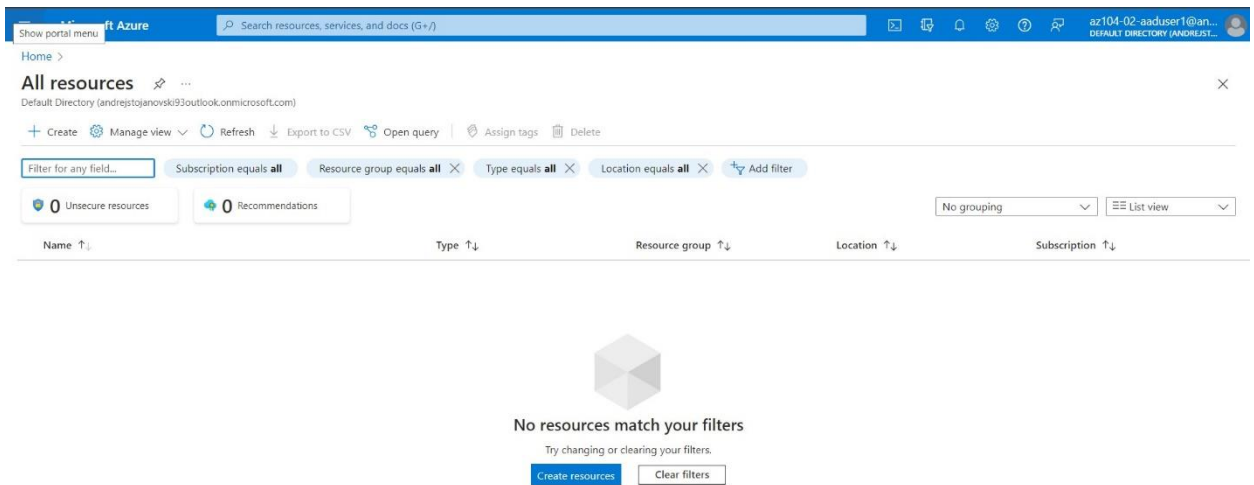
+ Create Manage view Refresh Export to CSV Open query Assign tags

Filter for any field... Subscription equals all Location equals all Add filter

0 Unsecure resources 0 Recommendations No grouping List view

Name	Subscription	Location
cloud-shell-storage-westeuropa	Azure Pass - Sponsorship	West Europe
NetworkWatcherRG	Azure Pass - Sponsorship	East US

2. In the **InPrivate** browser window, in the Azure portal, search and select **All resources** to verify that the az104-02-aaduser1 user cannot see any resources.



Home > All resources

Default Directory (andrejstojanovski93outlook.onmicrosoft.com)

+ Create Manage view Refresh Export to CSV Open query Assign tags Delete

Filter for any field... Subscription equals all Resource group equals all Type equals all Location equals all Add filter

0 Unsecure resources 0 Recommendations No grouping List view

Name Type Resource group Location Subscription

No resources match your filters

Try changing or clearing your filters.

Create resources Clear filters