

**Міністерство освіти і науки України
Карпатський національний університет
імені В.Стефаника**

Факультет математики та інформатики
Кафедра інформаційних технологій

Хмарні технології

Практична робота №2а

Тема: Manage Subscriptions and RBAC

Мета: Навчитися керуванню контролем, основаному на ролях

Виконав: Андрусяк І.Р.
Група ПІЗ-41
Дата: 25 листопада 2025р.
Викладач: Поварчук Д.Д.

Task 1: Implement Management Groups

```
23  ✓ resource "azurerm_management_group" "az104_mg1" {
24      name          = "az104-mg1"
25      display_name = "az104-mg1"
26  }
```

Task 2: Review and assign a built-in Azure role


```
28  resource "azuread_group" "helpdesk" {
29      display_name = "helpdesk"
30      owners       = [data.azurerm_client_config.current.object_id]
31      security_enabled = true
32  }
33
34  resource "azurerm_role_assignment" "vm_contributor_helpdesk" {
35      scope                = azurerm_management_group.az104_mg1.id
36      role_definition_name = "Virtual Machine Contributor"
37      principal_id         = azuread_group.helpdesk.object_id
38  }
```


Task 3: Create a custom RBAC role

```
40  resource "azurerm_role_definition" "custom_support_request" {
41      name          = "Custom Support Request"
42      scope         = azurerm_management_group.az104_mg1.id
43      description   = "A custom contributor role for support requests."
44
45      permissions {
46          actions = [
47              "Microsoft.Support/supportTickets/read",
48              "Microsoft.Support/supportTickets/write",
49              "Microsoft.Resources/subscriptions/resourceGroups/read",
50              "Microsoft.Resources/subscriptions/read"
51          ]
52
53          not_actions = [
54              "Microsoft.Support/register/action"
55          ]
56      }
57
58      assignable_scopes = [
59          azurerm_management_group.az104_mg1.id
60      ]
61  }
```










Task 4: Monitor role assignments with the Activity Log

Looking for Log Analytics? In Log Analytics you can search for performance, diagnostics, health logs, and more. [Visit Log Analytics](#)

Search  Quick Insights

Management Group : **az104-mg1** Subscription : **None** Event severity : **All** Timespan : **Last 6 hours**  Add Filter

9 items.

Operation name	Status	Time	Time stamp	Subscription
▼  Create or update custom role definition	Succeeded	15 minutes ...	Tue Nov 25 ...	
 Create or Update	Started	16 minutes ...	Tue Nov 25 ...	
 Create or Update	Accepted	16 minutes ...	Tue Nov 25 ...	
 Create role assignment	Started	16 minutes ...	Tue Nov 25 ...	
 Create role assignment	Succeeded	16 minutes ...	Tue Nov 25 ...	
 Create or Update	Succeeded	16 minutes ...	Tue Nov 25 ...	
 Create role assignment	Started	15 minutes ...	Tue Nov 25 ...	
 Create or update custom role definition	Started	15 minutes ...	Tue Nov 25 ...	
 Create role assignment	Succeeded	15 minutes ...	Tue Nov 25 ...	

Висновок

У ході лабораторної роботи було практично реалізовано модель безпеки Azure "зверху вниз". Хоча використання Terraform для управління ідентифікаторами та групами керування іноді вимагає додаткових налаштувань у графічному інтерфейсі, цей підхід довів свою перевагу в швидкості розгортання кількох однотипних середовищ.

Робота підтвердила важливість механізму успадкування (inheritance): права, призначені на рівні групи керування, автоматично каскадуються на всі ресурси нижчих рівнів, що значно знижує адміністративне навантаження. Створення кастомних ролей дозволило точно налаштувати дозволи (Microsoft.Support/*), усуваючи надлишкові права, які зазвичай мають вбудовані ролі.

Гітхаб: https://github.com/Illoizaur/azure_labs/tree/main/lab2