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 ІПЗ-41
Дата: 25 листопада 2025р.
Викладач: Поварчук Д.Д.

Івано-Франківськ — 2025

Task 1: Implement Management Groups

```
resource "azurerm_management_group" "az104_mg1" {
  name         = "az104-mg1"
  display_name = "az104-mg1"
}
```

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

```
resource "azuread_group" "helpdesk" {
  display_name     = "helpdesk"
  owners           = [data.azurerm_client_config.current.object_id]
  security_enabled = true
}

resource "azurerm_role_assignment" "vm_contributor_helpdesk" {
  scope                = azurerm_management_group.az104_mg1.id
  role_definition_name = "Virtual Machine Contributor"
  principal_id         = azuread_group.helpdesk.object_id
}
```

Task 3: Create a custom RBAC role

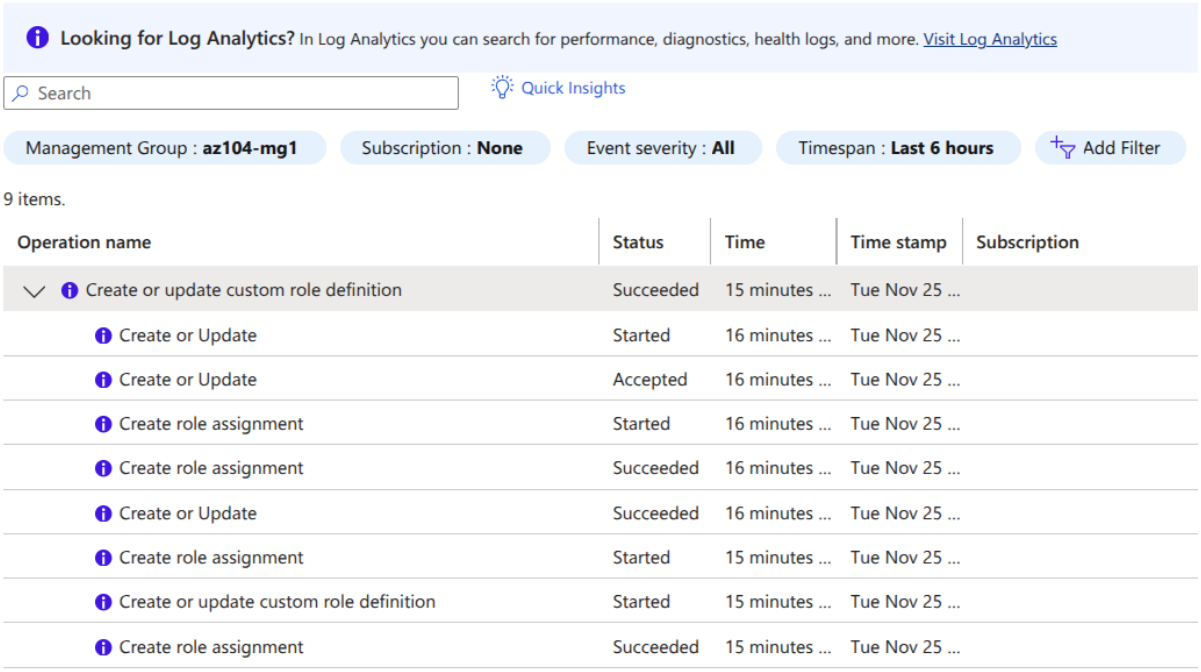
```
resource "azurerm_role_definition" "custom_support_request" {
  name        = "Custom Support Request"
  scope       = azurerm_management_group.az104_mg1.id
  description = "A custom contributor role for support requests."

  permissions {
    actions = [
      "Microsoft.Support/supportTickets/read",
      "Microsoft.Support/supportTickets/write",
      "Microsoft.Resources/subscriptions/resourceGroups/read",
      "Microsoft.Resources/subscriptions/read"
    ]

    not_actions = [
      "Microsoft.Support/register/action"
    ]
  }

  assignable_scopes = [
    azurerm_management_group.az104_mg1.id
  ]
}
```

Task 4: Monitor role assignments with the Activity Log



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