

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

**Факультет математики та інформатики
Кафедра інформаційних технологій**

Хмарні технології

Практична робота № 1

Тема: Manage Microsoft Entra ID Identities

Мета: Навчитися створювати та керувати обліковими записами користувачів і групами у Microsoft Entra ID.

Виконав: Андрусак І.Р.

Група ІПЗ-41

Дата: 26 вересня 2025р.

Викладач: Поварчук Д.Д.

Мета лабораторної: «Ваша організація створює нове лабораторне середовище для попереднього тестування додатків і служб. Для управління лабораторним середовищем, включаючи віртуальні машини, наймається кілька інженерів. Щоб інженери могли пройти автентифікацію за допомогою Microsoft Entra ID, вам доручено налаштувати користувачів і групи. Щоб мінімізувати адміністративні витрати, членство в групах має оновлюватися автоматично на основі посад.»

Завдання

Завдання 1: Створити та налаштувати облікові записи користувачів

1.1 Створити нового користувача

Створіть нового користувача з такими налаштуваннями (інші залиште за замовчуванням):

Setting	Value
User principal name	az104-user1
Display name	az104-user1
Auto-generate password	checked
Account enabled	checked
Job title (Properties tab)	IT Lab Administrator
Department (Properties tab)	IT
Usage location (Properties tab)	United States

Виконання завдання:

```
nvim
13 resource "random_password" "internal_user" {
12 |   length = 16
11 |   special = true
10 }
9
8 resource "azuread_user" "internal" {
7 |   user_principal_name = "${var.internal_alias}@${var.tenant_domain}"
6 |   display_name        = var.internal_alias
5 |   mail_nickname       = var.internal_alias
4
3 |   account_enabled     = true
2 |   password             = random_password.internal_user.result
1 |   force_password_change = true
14 |
1 |   job_title           = "IT Lab Administrator"
2 |   department          = "IT"
3 |   usage_location      = "US"
4 | }
```

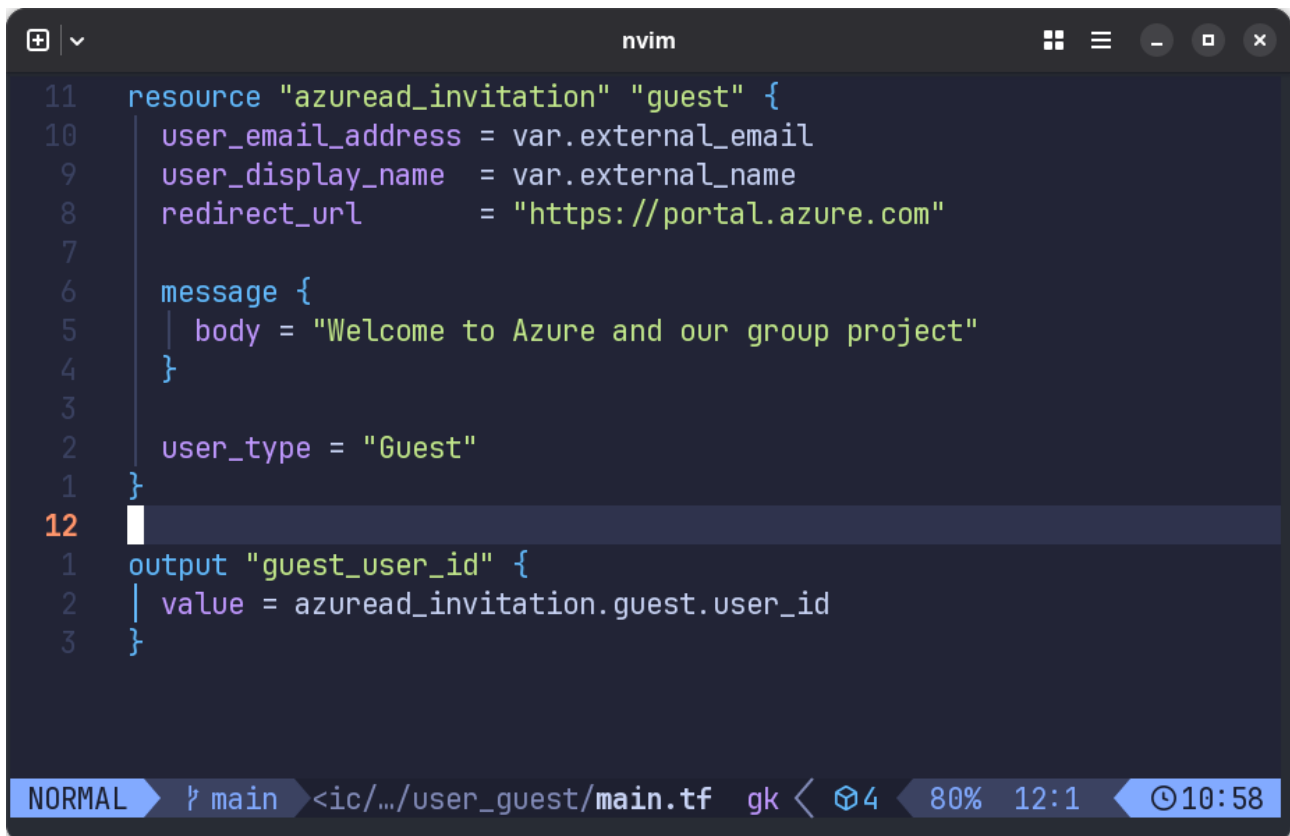
NORMAL | ? main | <.../user_internal/main.tf | gk | 4 | 63% | 14:1 | 10:58

1.2 Запросити зовнішнього користувача

In the **New user** drop-down select **Invite an external user**.

Setting	Value
Email	your email address
Display name	your name
Send invite message	check the box
Message	Welcome to Azure and our group project

Виконання:



```
11 resource "azuread_invitation" "guest" {
10   user_email_address = var.external_email
9    user_display_name = var.external_name
8    redirect_url      = "https://portal.azure.com"
7
6    message {
5      | body = "Welcome to Azure and our group project"
4    }
3
2    user_type = "Guest"
1  }
12
1  output "guest_user_id" {
2    | value = azuread_invitation.guest.user_id
3  }
```

NORMAL main <ic/.../user_guest/main.tf gk 4 80% 12:1 10:58




Далі я стикнувся з певними проблемами щодо зміни properties гостьового користувача до його прийняття запрошення. Тож цей крок:

2. Move to the **Properties** tab. Complete the basic information, including these fields.

Setting	Value
Job title	IT Lab Administrator
Department	IT
Usage location (Properties tab)	United States

Було виконано у графічному інтерфейсі, бо раз вже не вийшло повністю у тераформі, бавитись з скриптами бажання нема жодного. (детальніше про проблему можна почитати тут: <https://github.com/hashicorp/terraform-provider-azuread/issues/650>)

Знімка екрану після виконання завдання:

<input type="checkbox"/>	Display name ↑	User principal name ↑↓	User type	On-premises sy...	Identities	Company name	Creation type
<input type="checkbox"/>	 A.I.	andrusiakilla_gmai... 	Guest	No	05illiandrusgmail.onmicr...		Invitation
<input type="checkbox"/>	 az104-user1	az104-user1@05il... 	Member	No	05illiandrusgmail.onmicr...		
<input type="checkbox"/>	 Illia Andrusiak	05illiandrus_gmai... 	Member	No	MicrosoftAccount		Invitation

Завдання 2: Створити групи та додати учасників

Створіть групу із заданими параметрами, та призначте себе її власником:

Setting	Value
Group type	Security
Group name	<input type="text" value="IT Lab Administrators"/>
Group description	<input type="text" value="Administrators that manage the IT lab"/>
Membership type	Assigned

```

16 data "azuread_client_config" "current" {}
15
14 resource "azuread_group" "it_lab_administrators" {
13     display_name      = "IT Lab Administrators"
12     description       = "Administrators that manage the IT lab"
11     security_enabled  = true
10     mail_enabled      = false
9       assignable_to_role = false
8
7     owners = [data.azuread_client_config.current.object_id]
6
5     mail_nickname = "it-lab-administrators"
4 }
3
2 output "group_id" {
1     value = azuread_group.it_lab_administrators.object_id
17 }


```

Додайте до групи користувачів створених у кроці 1:

```
nvim
group/main.tf x | group_m.../main.tf x
1 resource "azuread_group_member" "internal_member" {
2   group_object_id = var.group_id
3   member_object_id = var.internal_user_id
4 }
5 resource "azuread_group_member" "guest_member" {
6   group_object_id = var.group_id
7   member_object_id = var.guest_user_id
8 }
NORMAL main <roup_membership/main.tf gk < 4 Top 1:1 11:01
```

Результат виконання:

Basic information

 **IT Lab Administrators**

Administrators that manage the IT lab

Membership type	Assigned	Total direct members	2
Source	Cloud	User(s)	2
Type	Security	Group(s)	0
Object ID	8559075f-8bd2-4d1f-8d83-b5c3fb947b58	Device(s)	0
Created on	9/26/2025, 3:50 PM	Other(s)	0

Feed

**Group memberships**
0
[View group memberships](#)

**Owners**
1
[View group owners](#)

**Total members**
2
[View group members](#)

Виводи з терміналу:

```
~/.Public/azure_labs/lab1

[illoi@archlinux lab1]$ terraform plan
module.it_group.data.azuread_client_config.current: Reading...
module.it_group.data.azuread_client_config.current: Read complete after 0s [id=f4392401-abd0-4c7d-b0e1-1a95b05d153d-04b07795-8ddb-461a-bbee-02f9e1bf7b46-06800f92-3136-4abc-9485-541a84bb21e1]

Terraform used the selected providers to generate the following
execution plan. Resource actions are indicated with the following
symbols:
  + create

Terraform will perform the following actions:

# module.group_membership.azuread_group_member.guest_member will be created
+ resource "azuread_group_member" "guest_member" {
  + group_object_id = (known after apply)
  + id              = (known after apply)
  + member_object_id = (known after apply)
}

# module.group_membership.azuread_group_member.internal_member will be created
+ resource "azuread_group_member" "internal_member" {
  + group_object_id = (known after apply)
  + id              = (known after apply)
  + member_object_id = (known after apply)
}

# module.guest_user.azuread_invitation.guest will be created
+ resource "azuread_invitation" "guest" {
  + id              = (known after apply)
  + redeem_url      = (known after apply)
  + redirect_url    = "https://portal.azure.com"
  + user_display_name = "A.I."
  + user_email_address = "andrusiakilla@gmail.com"
  + user_id         = (known after apply)
  + user_type       = "Guest"
}
```

```
~/.Public/azure_labs/lab1

run "terraform apply" now.
[illoi@archlinux lab1]$ terraform apply
module.it_group.data.azuread_client_config.current: Reading...
module.it_group.data.azuread_client_config.current: Read complete after 0s [id=f4392401-abd0-4c7d-b0e1-1a95b05d153d-04b07795-8ddb-461a-bbee-02f9e1bf7b46-06800f92-3136-4abc-9485-541a84bb21e1]

Terraform used the selected providers to generate the following
execution plan. Resource actions are indicated with the following
symbols:
  + create

Terraform will perform the following actions:

# module.group_membership.azuread_group_member.guest_member will be created
+ resource "azuread_group_member" "guest_member" {
  + group_object_id = (known after apply)
  + id              = (known after apply)
  + member_object_id = (known after apply)
}

# module.group_membership.azuread_group_member.internal_member will be created
+ resource "azuread_group_member" "internal_member" {
  + group_object_id = (known after apply)
  + id              = (known after apply)
  + member_object_id = (known after apply)
}

# module.guest_user.azuread_invitation.guest will be created
+ resource "azuread_invitation" "guest" {
  + id              = (known after apply)
  + redeem_url      = (known after apply)
  + redirect_url    = "https://portal.azure.com"
  + user_display_name = "A.I."
  + user_email_address = "andrusiakilla@gmail.com"
  + user_id         = (known after apply)
}
```

```
~/Public/azure_labs/lab1

Do you want to perform these actions?
Terraform will perform the actions described above.
Only 'yes' will be accepted to approve.

Enter a value: yes

module.internal_user.random_password.internal_user: Creating...
module.internal_user.random_password.internal_user: Creation complete after 0s [id=none]
module.guest_user.azuread_invitation.guest: Creating...
module.it_group.azuread_group.it_lab_administrators: Creating...
module.internal_user.azuread_user.internal: Creating...
module.internal_user.azuread_user.internal: Creation complete after 1s [id=09557421-b102-44bf-b94c-fcefd10f2dde]
module.guest_user.azuread_invitation.guest: Creation complete after 5s [id=7c332177-5ec6-45ef-a376-3d75f4df844e]
module.it_group.azuread_group.it_lab_administrators: Still creating... [00m10s elapsed]
module.it_group.azuread_group.it_lab_administrators: Still creating... [00m20s elapsed]
module.it_group.azuread_group.it_lab_administrators: Creation complete after 26s [id=24be2992-a97e-4a12-a9a5-43bba9e76fa2]
module.group_membership.azuread_group_member.internal_member: Creating...
module.group_membership.azuread_group_member.guest_member: Creating...
module.group_membership.azuread_group_member.internal_member: Creation complete after 1s [id=24be2992-a97e-4a12-a9a5-43bba9e76fa2/member/09557421-b102-44bf-b94c-fcefd10f2dde]
module.group_membership.azuread_group_member.guest_member: Creation complete after 1s [id=24be2992-a97e-4a12-a9a5-43bba9e76fa2/member/5a73a7b4-dcb6-490c-bcea-79b98961dbd4]

Apply complete! Resources: 6 added, 0 changed, 0 destroyed.

Outputs:

group_id = "24be2992-a97e-4a12-a9a5-43bba9e76fa2"
group_members = {
  "guest" = "5a73a7b4-dcb6-490c-bcea-79b98961dbd4"
  "internal" = "09557421-b102-44bf-b94c-fcefd10f2dde"
}
guest_user_id = "5a73a7b4-dcb6-490c-bcea-79b98961dbd4"
internal_user_id = "09557421-b102-44bf-b94c-fcefd10f2dde"
[iloi@archlinux lab1]$
```

Висновки

У ході роботи було реалізовано завдання з налаштування лабораторного середовища Microsoft Entra ID. Використання Terraform для управління хмарними ідентифікаторами дозволило глибше зрозуміти структуру об'єктів `azuread_user`, `azuread_invitation` та `azuread_group`.

Робота підтвердила, що IaC-підхід є ефективним для масового створення користувачів та груп, проте він має певні обмеження при взаємодії з гостьовими обліковими записами на етапі до прийняття запрошення. Покликання на репозиторій гітхаб:

https://github.com/Illoizaur/azure_labs/tree/main/lab1