

Міністерство науки і освіти України



**Звіт з лабораторної роботи №5
з дисципліни “Аналіз Програмного Забезпечення”**

Виконав:

Студент гр. 123-21-2

Манін Б.М.

Перевірив:

Асистент каф. САУ

Шевченко Ю.О.

Дніпро 2024

Лабораторна робота №5

Було запущено EC2 та обрано операційну систему Windows (рис.1).

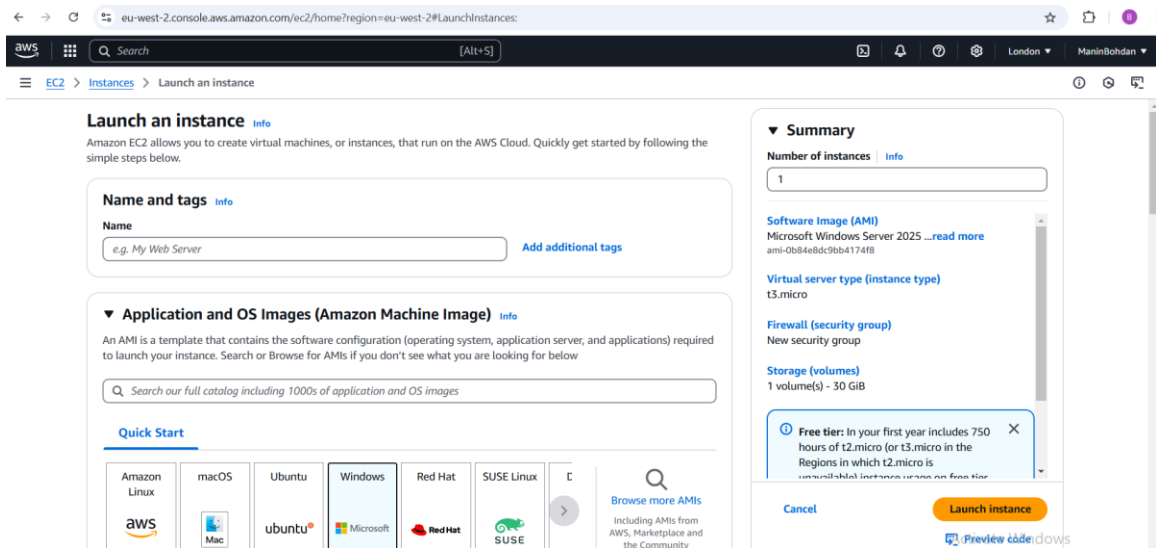


Рисунок 1 – Запуск EC2.

У якості операційної системи було обрано Windows Server 2022 Base.

Було обрано тип instance (рис. 2).

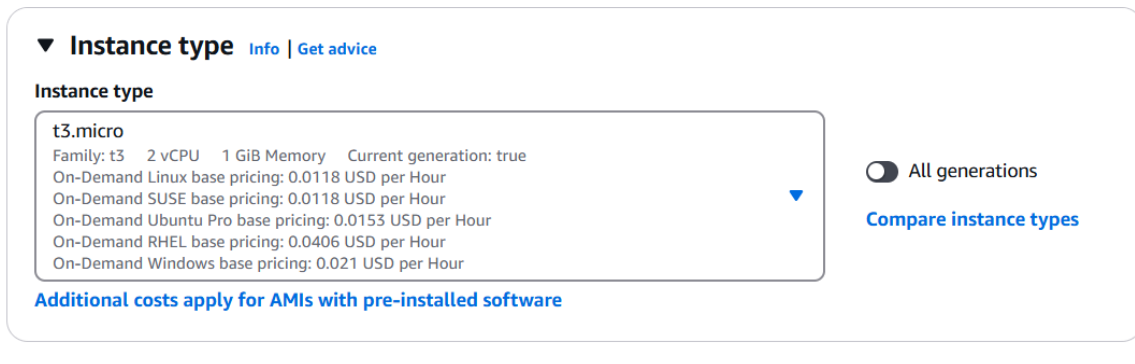


Рисунок 2 – Tun instance.

Було створено новий ключ доступу (рис.3).

Create key pair

Key pair name

Key pairs allow you to connect to your instance securely.

Enter key pair name

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type



☒ RSA
RSA encrypted private and public key pair

☐ ED25519
ED25519 encrypted private and public key pair (Not supported for Windows instances)

Private key file format

☒ .pem
For use with OpenSSH

☐ .ppk
For use with PuTTY

 When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more](#) 

Cancel

Create key pair

Рисунок 3 – Створення ключа доступу.

Мережеві налаштування мають наступний вигляд (рис.4).

▼ Network settings

Info

Edit

Network

Info

vpc-01819d1261b50fab8

Subnet

Info

No preference (Default subnet in any availability zone)

Auto-assign public IP

Info

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups)

Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group

Select existing security group

We'll create a new security group called 'launch-wizard-1' with the following rules:

☒ Allow RDP traffic from

Helps you connect to your instance

Anywhere
0.0.0.0/0

☐ Allow HTTPS traffic from the internet

To set up an endpoint, for example when creating a web server

☐ Allow HTTP traffic from the internet

To set up an endpoint, for example when creating a web server

⚠

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

×

Рисунок 4 – Мережеві налаштування.

Було запущено instance (рис. 5).

Instances (1)

Info

Last updated less than a minute ago

Connect

Instance state

Actions

Launch instances

Find Instance by attribute or tag (case-sensitive)

All states

Instance ID = i-06c74f3dc3d50c678

Clear filters

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
<input type="checkbox"/>		i-06c74f3dc3d50c678	Running	t3.micro	Initializing	View alarms	eu-west-2b	ec2-

Рисунок 5 – Запуск instance.

Далі було отримано пароль адміністратора, за допомогою завантаження .pem файлу (рис. 6-7).

Get Windows password [info](#)

Use your private key to retrieve and decrypt the initial Windows administrator password for this instance.

Instance ID
i-06c74f3dc3d50c678

Key pair associated with this instance
Manin-Bohdan_key

Private key
Either upload your private key file or copy and paste its contents into the field below.

[Upload private key file](#)

Manin-Bohdan_key.pem
1.674KB

Private key contents - optional

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA2sxREdO3F1OYjhsryqun92M+9hdo5ppLt1X0rigOO/jlzWX
tmwjDul4MwPTJ4KBwPH84lnlqyUMsYDHVrtK1FzzmWU/r4QA4Xx7+3dPRH3TZW
BzF5cO5xkfRmjX+5aDi8nUTvpK6eFw8fANrY95mywdnhqVti69PPj7Z2ylwjhCFX
/KUBJdONTmbnBiSEwVIMbNTDqAVhpMdv7FKhalSwBpJBGGZMG5JTj8DTI/525//6a
iNSewJERH5TaEPriertQqLibGLzMv00lga+k04w+tbvbgV1N4xELuDFIMPwrz8v
oTeLmLr4SnINRWssgrsG7VGQLU5JZL3Zj4gfOWIDAQABAoIBACaRHTknOH7EHX/v
CikOpZliVDGQUfEkptLb8T8TJEVIA7YDnFprdUKLpMRZTNRKDNUVOp2Tdeu0/CFN
-----
```

[Cancel](#) [Decrypt password](#) [Activate Windows](#)

Рисунок 6 – Отримання паролю адміністратора.

Public DNS

ec2-13-41-53-173.eu-west-2.compute.amazonaws.com

Password

m10x\$o&n-Q?kUQa*.9ffKTPBZCu*99pB

Рисунок 7 – Отримання паролю адміністратора.

Було запущено віртуальну машину та змінено зображення робочого стола (рис.8).

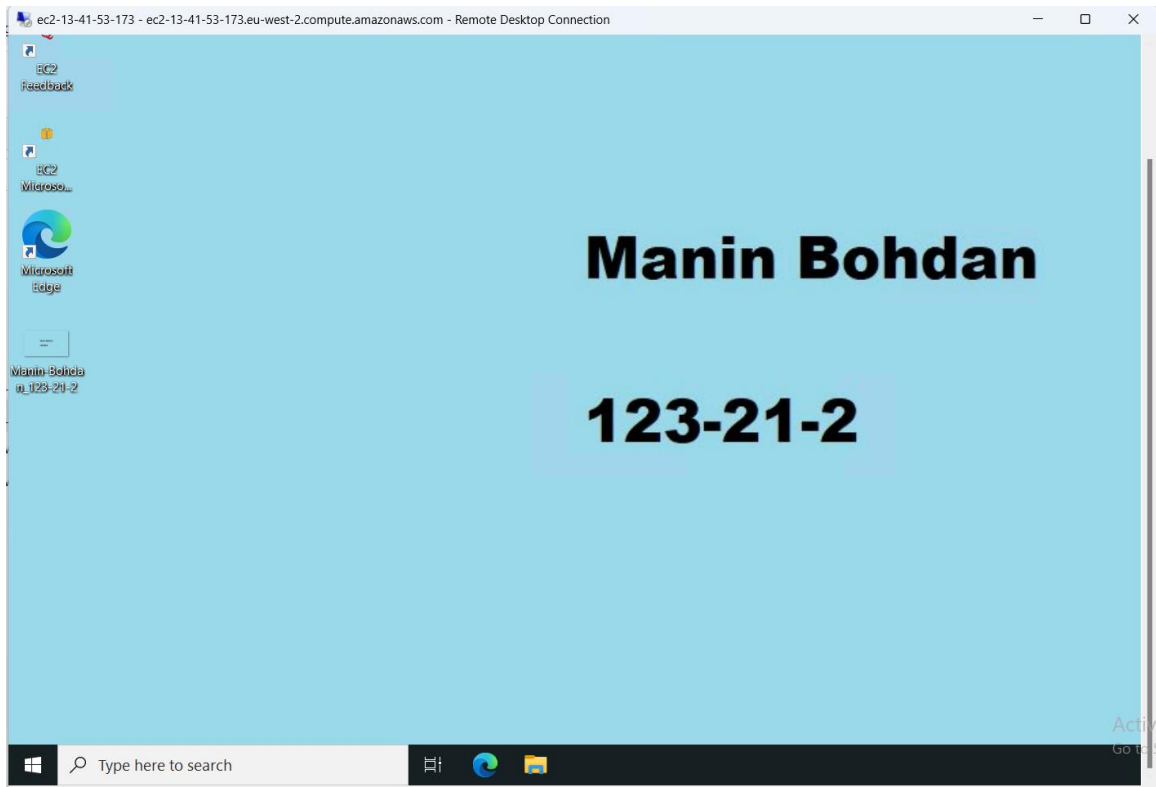


Рисунок 8 – Запуск віртуальної машини

Результатом виконання роботи є:

Публічна IP-адреса ВМ - 13.41.53.173

Пароль адміністратора - m1Ox\$o&n-Q?kUQa*.9ffKTPBZCu*99pB