

**Міністерство освіти і науки України**

**Національний технічний університет «Дніпровська політехніка»**



**Звіт**

**Лабораторна робота №5**

**З дисципліни «Аналіз програмного забезпечення»**

**Виконала:**

**студентка групи 122-22-5**

**Алексєєнко Є.Д.**

**Перевірив:**

**Мінєєв Олександр Сергійович**

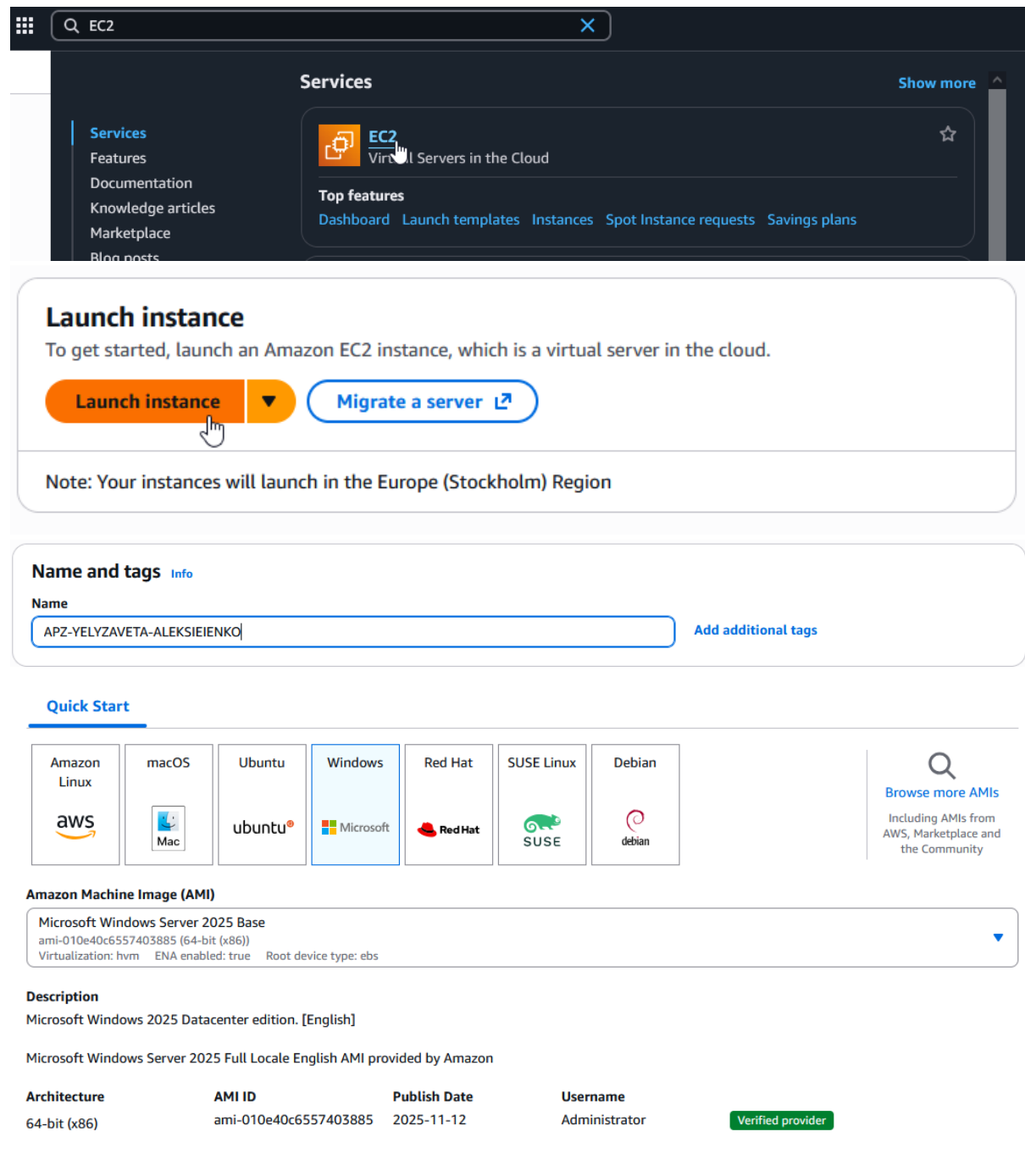
**Юлія Олександрівна Шевченко**

**м. Дніпро**

**2025 рік**

**Мета роботи:** набування навичок створення та розміщення віртуального сервера за допомогою AWS EC2.

Створюємо Instance. Для цього перейшла на [AWS Management Console](#) та увійшла за своїм обліковим записом AWS. У рядку пошуку консолі ввела EC2:



The screenshot shows the AWS Management Console interface. At the top, there is a search bar with 'EC2' entered. Below the search bar, the 'Services' section is visible, with 'EC2' selected. The main content area features a 'Launch instance' button and a 'Migrate a server' button. Below these buttons, a note states: 'Note: Your instances will launch in the Europe (Stockholm) Region'. The 'Name and tags' section shows a text input field with the value 'APZ-YELYZAVETA-ALEKSIEIENKO'. The 'Quick Start' section displays a grid of operating system logos: Amazon Linux, macOS, Ubuntu, Windows, Red Hat, SUSE Linux, and Debian. Below this, the 'Amazon Machine Image (AMI)' section shows a list of AMIs, with 'Microsoft Windows Server 2025 Base' selected. The 'Description' section provides details about the selected AMI, including its architecture, AMI ID, publish date, and username. A 'Verified provider' badge is also visible.

**Launch instance**

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

[Launch instance](#) [Migrate a server](#)

Note: Your instances will launch in the Europe (Stockholm) Region

**Name and tags** [Info](#)

Name

APZ-YELYZAVETA-ALEKSIEIENKO [Add additional tags](#)

**Quick Start**

Amazon Linux macOS Ubuntu Windows Red Hat SUSE Linux Debian

**Amazon Machine Image (AMI)**

Microsoft Windows Server 2025 Base  
ami-010e40c6557403885 (64-bit (x86))  
Virtualization: hvm ENA enabled: true Root device type: ebs

**Description**

Microsoft Windows 2025 Datacenter edition. [English]

Microsoft Windows Server 2025 Full Locale English AMI provided by Amazon

Architecture	AMI ID	Publish Date	Username
64-bit (x86)	ami-010e40c6557403885	2025-11-12	Administrator

Verified provider

Створюємо key pair:

## Create key pair

Key pair name

Key pairs allow you to connect to your instance securely.

apz-my-firstkey

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

apz-my-firstkey.pem

Открыть файл

Далі налаштовуємо Configure storage:

▼ Configure storage [Info](#)

Advanced

1x 30 GiB gp3 Root volume, 3000 IOPS, Not encrypted

Add new volume

The selected AMI contains instance store volumes, however the instance does not allow any instance store volumes. None of the instance store volumes from the AMI will be accessible from the instance

🕒 Click refresh to view backup information

The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

🔄

0 x File systems

Edit

▼ Summary

Number of instances | [Info](#)

1

⌵

Software Image (AMI)

Microsoft Windows Server 2025 ...[read more](#)

ami-010e40c6557403885

Virtual server type (instance type)

t3.micro

Firewall (security group)


New security group

Storage (volumes)

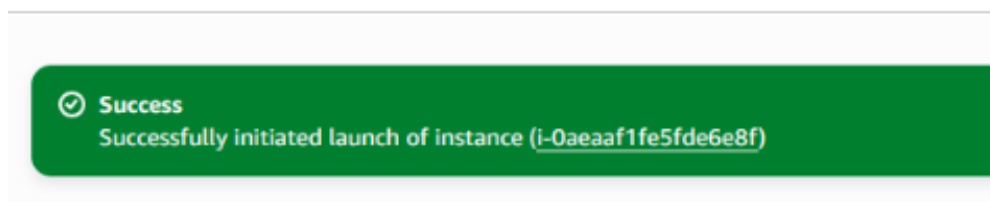
1 volume(s) - 30 GiB

Cancel

Launch instance

 [Preview code](#)

Instance був успішно створений:



Наступний крок - це отримання паролю Windows:

**Get Windows password**

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

Get Windows password

↗

## Get Windows password [info](#)

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

Instance ID  
[i-Oaeaf1fe5fde6e8f](#) (APZ-YELYZAVETA-ALEKSIEIENKO)

Key pair associated with this instance  
[apz-my-firstkey](#)

Private key

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

[Upload private key file](#)

apz-my-firstkey.pem  
1.67 KB

Private key contents

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAesh0bMV8pXqldJ4v5Ln9p/dDVa7qOHY3n1/rmQ+7Jfij
vApLFNZ5h8gPT0p4yT1PqYufWFCarEd91dgUBhq6s8vLpRz3zVApLPFDmgPDG
pUvb5Xf+m9UUVcPC/5mVFE84yFavnuJBm2Dh82dkd2Vj4M45fU13Gn78hBly
HCqhDfc7CBERaYrDPqxXilbilDrACLO7Migm41qBINe3f/JE2EAymKALMpJry5Kv
GxkJ8Jte8G7BRWRt9f4Tc6IW96JW+G2TWSlBNOCPJC1q1puqEsazM6MdeEM+Bx
Ra9z6reB1G2rira1DxsKKmGDlu5M36kc4kgKSQIDAQABAoIBAABb/ffBdgZ8BQB
MdcRj6FNL6G21/uow0y8byrRT86TQ27OLr6SuiMgiLN+t0RfWzfvOSJWBXDXD4i+7
-----
```

[Cancel](#)

[Decrypt password](#)

## Get Windows password

Connect to your Windows instance using Remote Desktop with this information.

**Instance ID**  
[i-Oaeaf1fe5fde6e8f](#) (APZ-YELYZAVETA-ALEKSIEIENKO)

**Private IP address**  
[\[REDACTED\]](#)

**Username**  
[Administrator](#)

**Password**  
[\[REDACTED\]](#)

**Password change recommended**

We recommend that you change your default password. Note: If a default password is changed, it cannot be retrieved using this tool. It is important that you change your password to one that you will remember.

[Cancel](#) [OK](#)

Password decryption successful  
The password for instance [i-Oaeaf1fe5fde6e8f](#) was successfully decrypted.

Instances (1) [info](#)

[Find Instance by attribute or tag \(case-sensitive\)](#) [All states](#)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs	Monitoring	Security group name	Key name
APZ-YELYZAV...	<a href="#">i-Oaeaf1fe5fde6e8f</a>	Running	t3.micro	1/3 checks pass	<a href="#">View alarms</a>	eu-north-1b	ec2-13-53-129-43.eu-n...	13.53.129.43	-	-	disabled	launch-wizard-1	apz-my-firstkey

Підключення до віддаленого комп'ютера (Windows EC2 Instance):

Після успішного створення віртуального сервера на AWS EC2 я виконала підключення до нього за допомогою віддаленого робочого столу (RDP).

1. Спочатку я отримала Public IP-адресу свого Instance у консолі AWS EC2.

**Public IPv4 address**

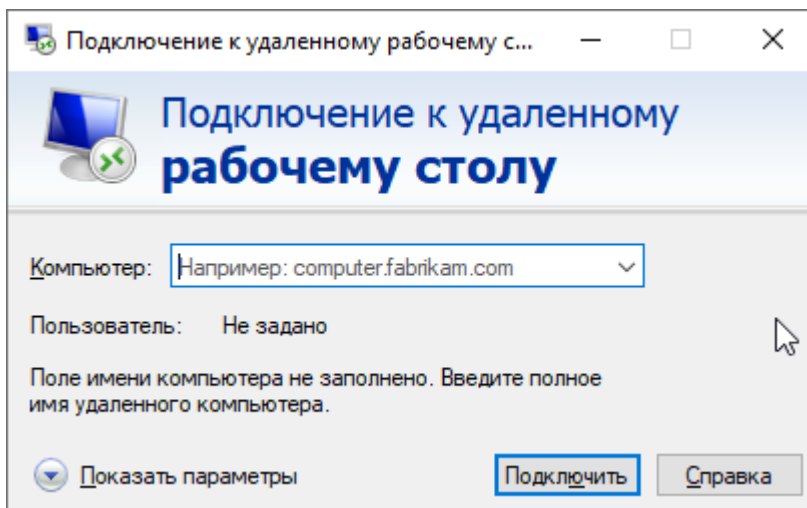
 13.53.129.43 | [open address](#) 

2. Далі натиснула Connect → RDP client → Get password, використавши свій Key Pair (.pem) для розшифрування паролю адміністратора.

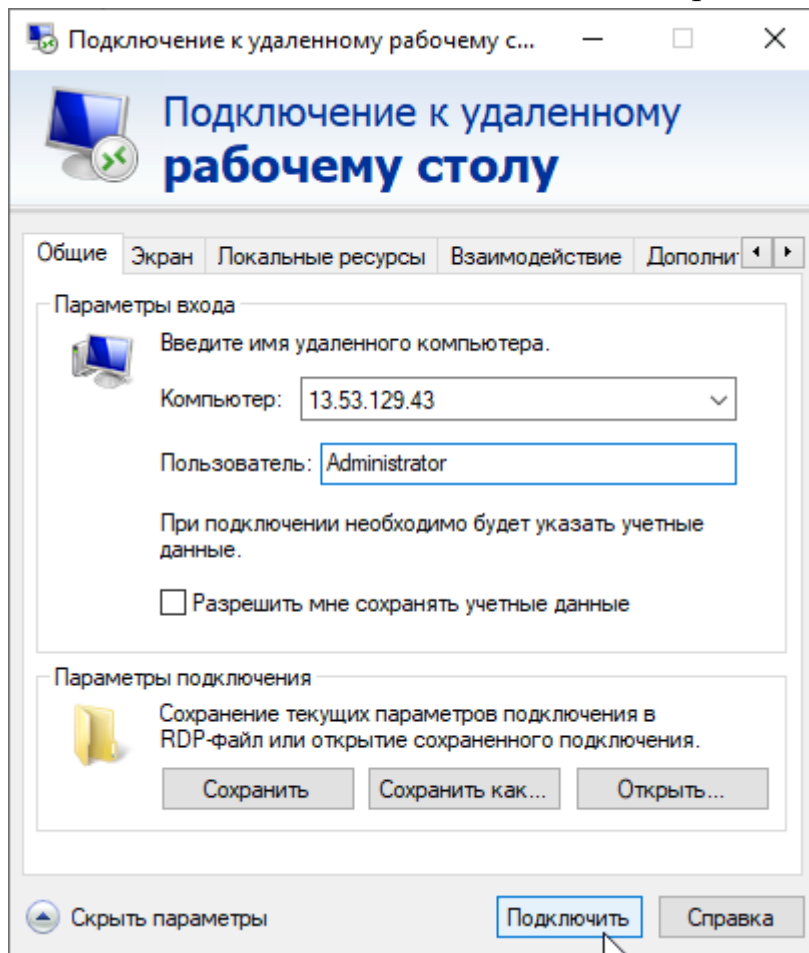
| Key name ▼ |

apz-my-firstkey

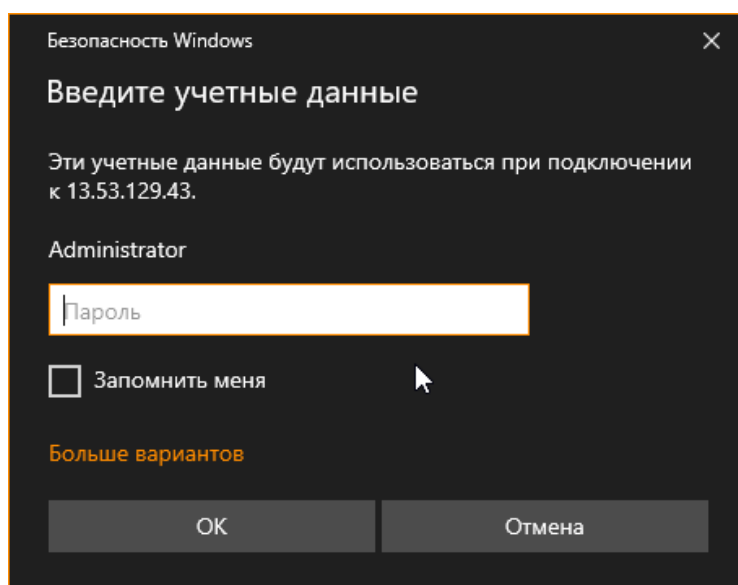
3. На своєму комп'ютері відкрила програму Підключення до віддаленого робочого столу (mstsc).

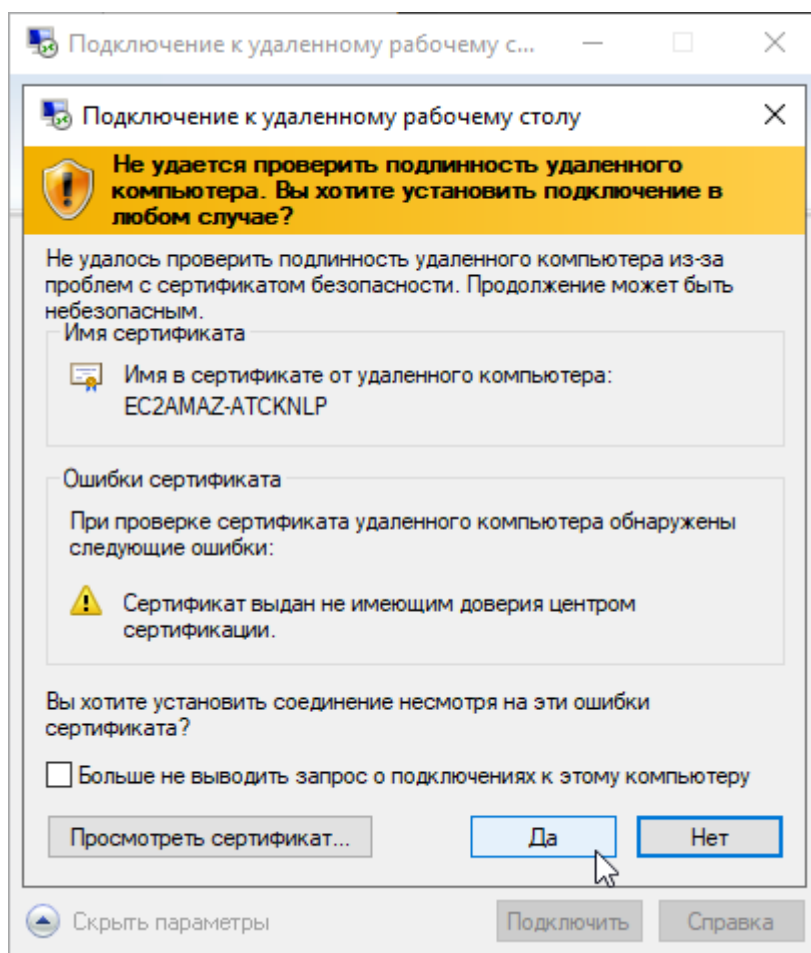
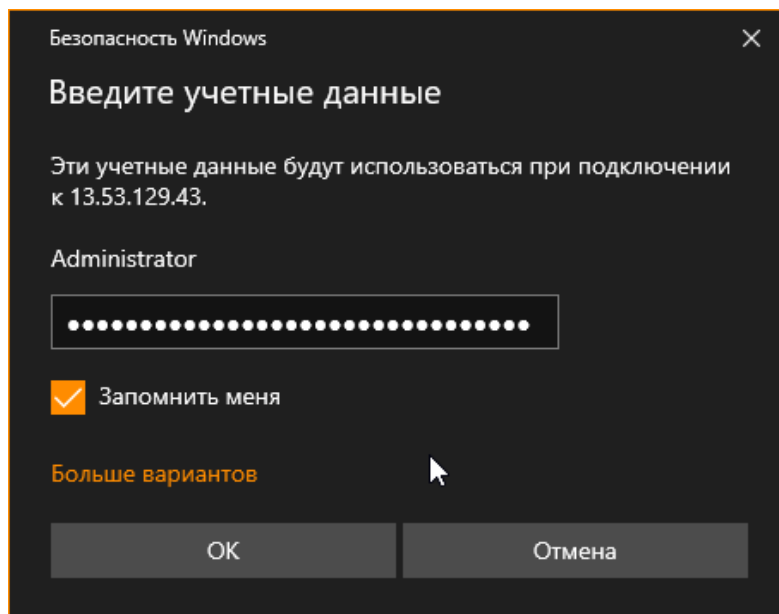


4. В полі Computer ввела Public IP свого сервера, а в полі Username — Administrator. У поле Password вставила пароль, отриманий на AWS.

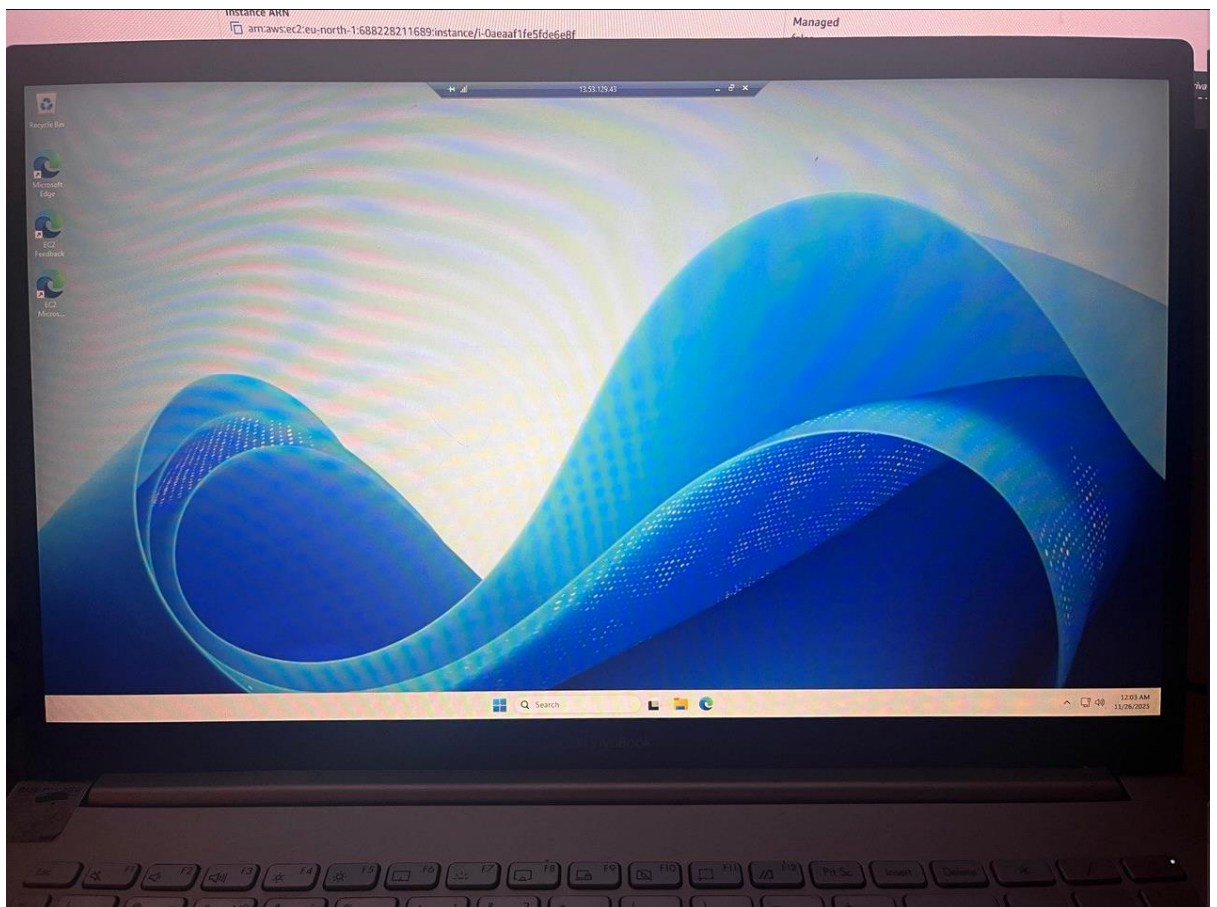
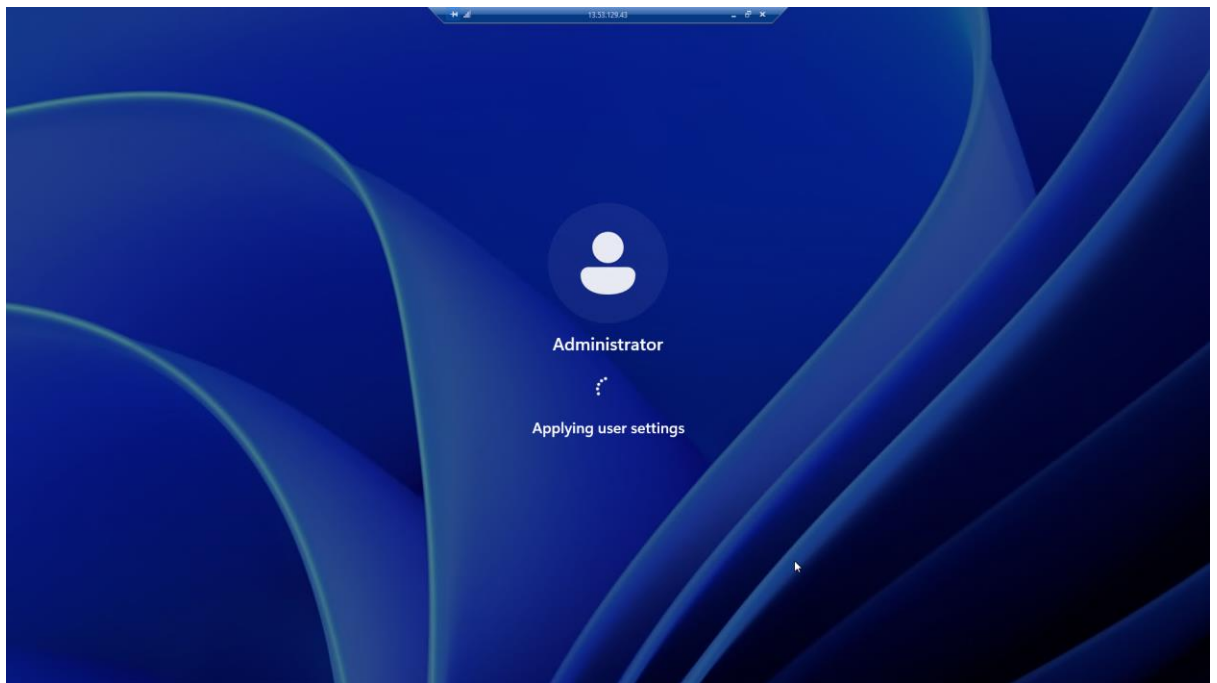


5. Натиснула Connect і підтвердила сертифікат безпеки, після чого відбулося успішне підключення до віддаленого робочого столу Windows.









Таким чином я змогла отримати доступ до свого EC2 Instance і готова виконувати подальші дії на сервері.

**Висновок:**

Під час виконання лабораторної роботи я ознайомилася з процесом створення та налаштування віртуального сервера на AWS EC2, включаючи створення key pair, налаштування сховища та отримання паролю адміністратора для Windows. Я успішно підключилася до віддаленого робочого столу та отримала доступ до сервера, що дозволяє виконувати подальші операції та тестування програмного забезпечення. Робота допомогла набути практичних навичок роботи з хмарними сервісами та віддаленими серверами.