

AWS Task-1

Task Description:

Create a Windows VM machine in AWS and connect with RDP open CMD in windows share the about system info.

Step 1: Login to AWS

Step 2: Create a Windows VM in AWS

Step 3: Connect using RDP and fetch the system information

- i) Using RDP (Pre-available in windows)
- ii) Using MobaXterm

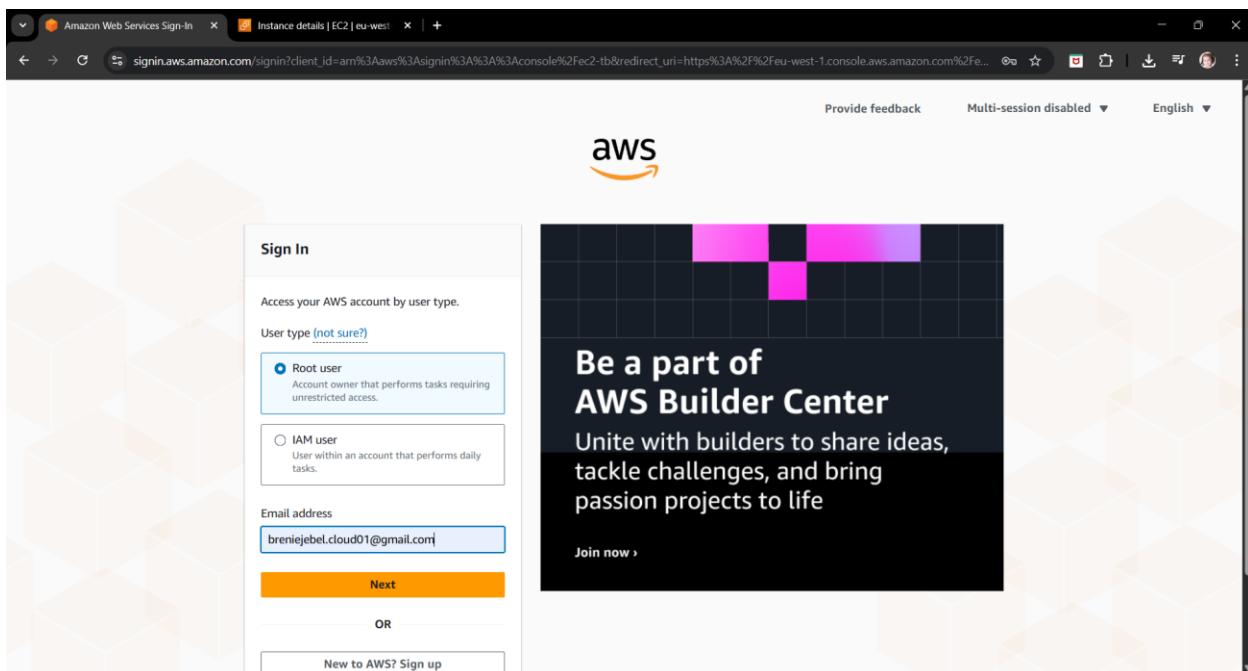
Step 4: Clean up

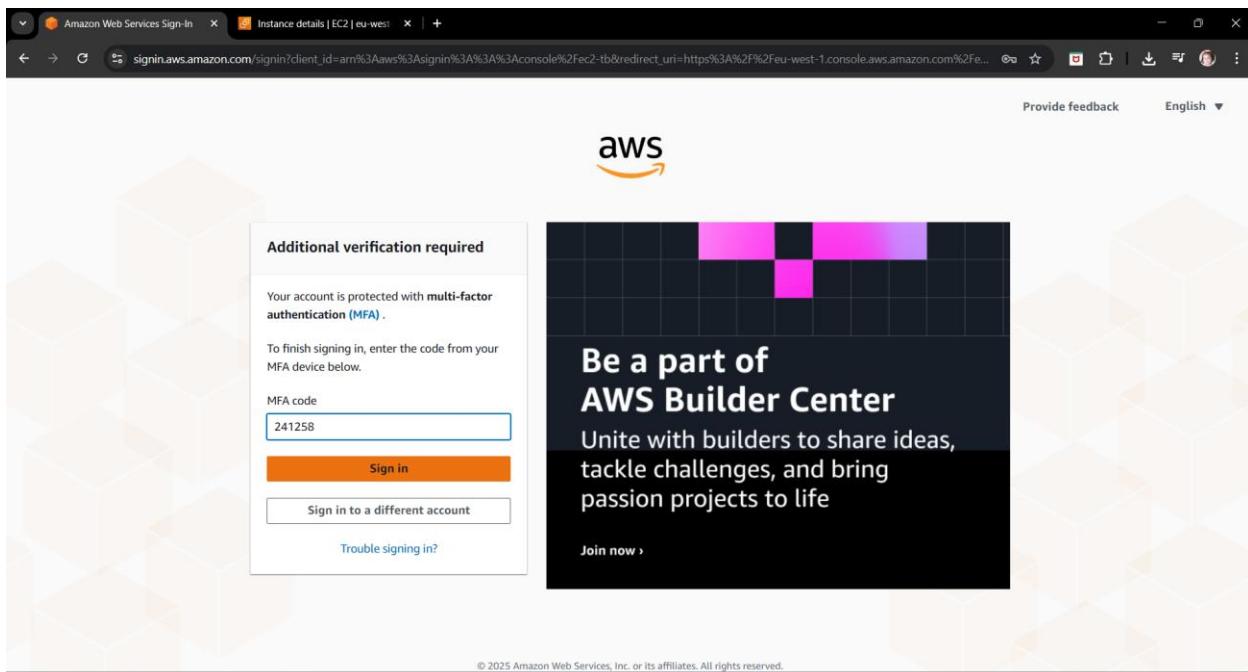
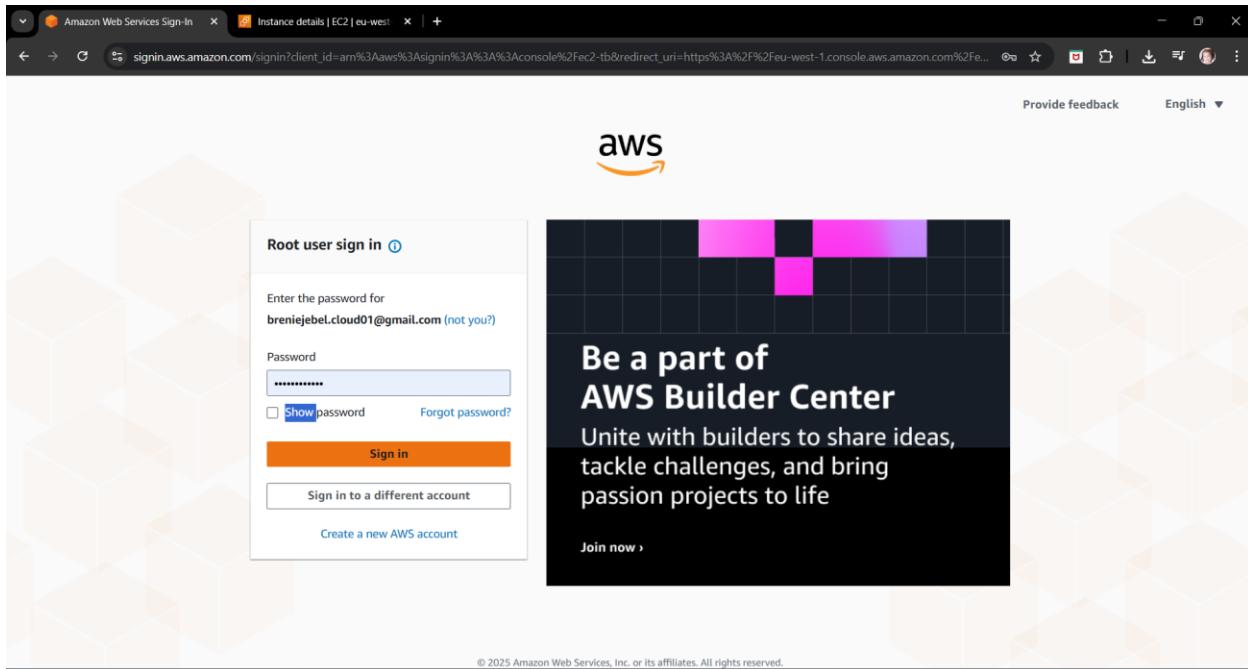
- i) Delete the created instance
- ii) Delete the created security group

Screenshots :

Step 1 : Login to AWS

A web browser was opened and the URL <https://console.aws.amazon.com> was entered. After signing in with AWS credentials, the EC2 Dashboard was opened to start working with virtual machines.





The screenshot shows the AWS Console Home page. On the left, there's a sidebar with 'Recently visited' services: EC2, Route 53, VPC, Lightsail, Aurora and RDS, Billing and Cost Management, Simple Notification Service, CloudWatch, S3, EFS, and Lambda. Below this is a 'View all services' link. To the right, there's a 'Applications' section with a 'Create application' button and a note about no applications. At the bottom, there are links for 'CloudShell', 'Feedback', and 'Console Mobile App'.

Step 2 : Create a Windows VM in AWS

Launch the Instance

From the EC2 Dashboard, the Launch Instance option was selected. The instance name was provided as “winServer01” during the configuration process.

The screenshot shows the EC2 Dashboard. On the left, there's a sidebar with 'Instances', 'Images', and 'Elastic Block Store' sections. The main area features a large 'Amazon Elastic Compute Cloud (EC2)' header with the subtext 'Create, manage, and monitor virtual servers in the cloud.' It includes a 'Launch a virtual server' box with 'Launch instance', 'View dashboard', and 'Get started walkthroughs' buttons, along with a 'Get started tutorial' link. Below this, there's a 'Benefits and features' section with a heading 'EC2 offers ultimate scalability and control' and a list of bullet points. To the right, there's an 'Additional actions' box with 'View running instances' and 'Migrate a server' links, and a 'Pricing (US)' section.

The screenshot shows the 'Launch an instance' wizard on the AWS EC2 console. The current step is 'Name and tags'. A message at the top says: 'It seems like you may be new to launching instances in EC2. Take a walkthrough to learn about EC2, how to launch instances and about best practices' with 'Take a walkthrough' and 'Do not show me this message again.' buttons. The main area shows a 'Name and tags' section where 'winServer01' is entered in the 'Name' field. Below it is a 'Software Image (AMI)' section showing 'Amazon Linux 2025 AMI 2023.9.2...'. The 'Virtual server type (instance type)' is set to 't3.micro'. Under 'Storage (volumes)', there is 1 volume(s) - 8 GiB. On the right, there are 'Cancel', 'Launch instance', and 'Preview code' buttons.

Select the AMI

For the operating system, the Microsoft Windows Server 2025 Base Amazon Machine Image (AMI) was chosen. This AMI provides a Windows Server environment suitable for RDP-based access.

The screenshot shows the 'Launch an instance' wizard on the AWS EC2 console. The current step is 'Application and OS Images (Amazon Machine Image)'. In the 'Recent' tab, 'Windows' is selected. The 'Quick Start' tab is also visible. The 'Amazon Machine Image (AMI)' section shows 'Microsoft Windows Server 2025 Base' as the selected item. Below it, details show: 'ami-0f4dbc4289c547d4d (64-bit (x86))', 'Virtualization: hvm', 'ENAv2 enabled: true', 'Root device type: ebs', and 'Free tier eligible'. To the right is a 'Summary' panel with 'Number of instances' set to 1, 'Software Image (AMI)' set to 'Microsoft Windows Server 2025 ...', 'Virtual server type (instance type)' set to 't3.micro', and 'Storage (volumes)' set to 1 volume(s) - 30 GiB. On the right, there are 'Cancel', 'Launch instance', and 'Preview code' buttons.

Select the Instance Type

The instance type was set to “t3.small”, which is eligible under the AWS Free Tier. This option is sufficient for testing and demonstration purposes.

This screenshot shows the 'Launch an instance' wizard on the AWS EC2 console. The current step is 'Instance type'. A 't3.small' instance is selected, which is described as 'Free tier eligible'. Other options like 'On-Demand Windows base pricing' and 'On-Demand Linux base pricing' are also listed. Below this, there's a note about additional costs for AMIs with pre-installed software. The 'Summary' section on the right shows one instance being launched with a Microsoft Windows Server 2025 AMI. The 'Launch instance' button is prominently displayed at the bottom right.

Create a Key Pair

A new key pair was created in order to securely access the instance. The .pem file generated during this step was downloaded and stored safely. This key is required later to decrypt the administrator password.

This screenshot shows the 'Launch an instance' wizard on the AWS EC2 console, currently at the 'Key pair (login)' step. A new key pair named 'Select' is chosen. The 'Summary' section on the right shows the same configuration as the previous step: one instance launching with a Microsoft Windows Server 2025 AMI. The 'Launch instance' button is again at the bottom right.

Launch an instance | EC2 | eu-west-1

eu-west-1.console.aws.amazon.com/ec2/home?region=eu-west-1#LaunchInstances:

aws Search [Alt+S]

EC2 Instances Launch an instance

Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

For Windows instances, you use a key pair to decrypt the administrator password. Then you use the decrypted password to connect to your instance.

Network settings Info

Network Info vpc-0f015a10b4b968d24

Subnet Info No preference (Default subnet in any availability zone)

Auto-assign public IP Info Enable

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance.

Create security group Select existing security group

We'll create a new security group called 'launch-wizard-2' with the following rules:

Allow RDP traffic from Anywhere (0.0.0.0/0)

Create key pair

Summary

Number of instances

Software Image (AMI) microsoft Windows Server 2025 ... read more

Virtual server type (instance type) t3.small

Firewall (security group) New security group

Storage (volumes) 1 volume(s) - 30 GiB

Launch instance Preview code

CloudShell Feedback Console Mobile App

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Launch an instance | EC2 | eu-west-1

eu-west-1.console.aws.amazon.com/ec2/home?region=eu-west-1#LaunchInstances:

aws Search [Alt+S]

EC2 Instances Launch an instance

Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

For Windows instances, you use a key pair to decrypt the administrator password. Then you use the decrypted password to connect to your instance.

Network settings Info

Network Info vpc-0f015a10b4b968d24

Subnet Info No preference (Default subnet in any availability zone)

Auto-assign public IP Info Enable

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-2' with the following rules:

Allow RDP traffic from Anywhere (0.0.0.0/0)

Create new key pair

Summary

Number of instances

Software Image (AMI) Microsoft Windows Server 2025 ... read more

Virtual server type (instance type) t3.small

Firewall (security group) New security group

Storage (volumes) 1 volume(s) - 30 GiB

Launch instance Preview code

CloudShell Feedback Console Mobile App

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Configure the Security Group

A new security group “launch-wizard-2” was created to allow remote access to the instance. The inbound rule for Remote Desktop Protocol (RDP) was configured to allow traffic from Anywhere (0.0.0.0/0) on port 3389, enabling RDP connectivity.

Network settings

Network: [Info](#)
vpc-0f015a10b4b968d24

Subnet: [Info](#)
No preference (Default subnet in any availability zone)

Auto-assign public IP: [Info](#)
Enable

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-2' with the following rules:

Allow RDP traffic from Anywhere (0.0.0.0/0)
Helps you connect to your instance

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.

Summary

Number of instances: [Info](#)
1

Software Image (AMI): Microsoft Windows Server 2025 ...[read more](#)
ami-0f4dbc4289c547d4d

Virtual server type (instance type): t3.small

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 30 GiB

[Cancel](#) [Launch instance](#) [Preview code](#)

This configuration allows RDP access from any source (0.0.0.0/0), which makes the instance accessible over RDP from any location.

Configure Storage

The root volume storage was configured with a size of 50 GiB using the gp3 volume type.

Configure storage

Advanced

1x 50 GiB 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

Advanced details

Summary

Number of instances: [Info](#)
1

Software Image (AMI): Microsoft Windows Server 2025 ...[read more](#)
ami-0f4dbc4289c547d4d

Virtual server type (instance type): t3.small

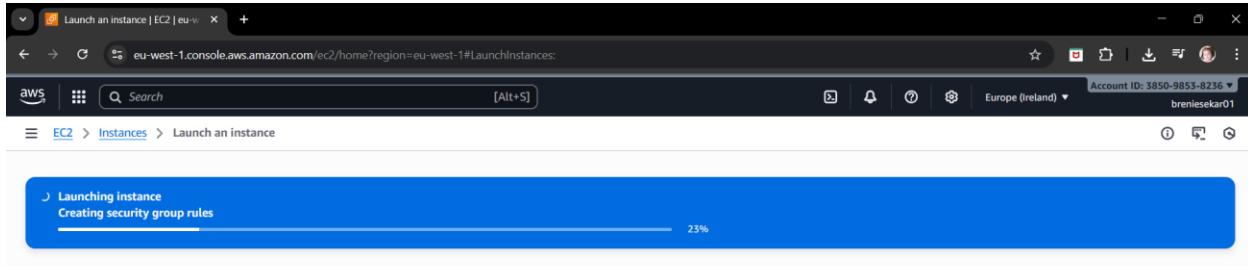
Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 50 GiB

[Cancel](#) [Launch instance](#) [Preview code](#)

Launch the Instance

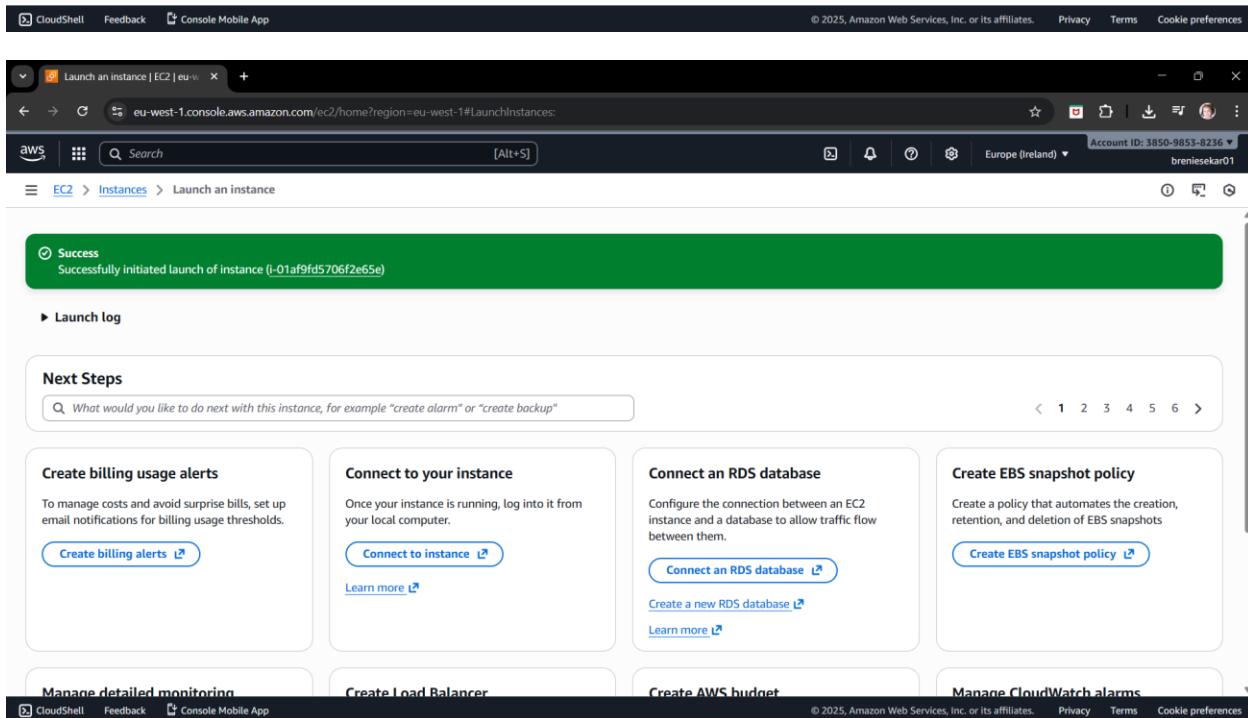
After launching, the instance appeared in the EC2 console and its status changed to Running.



The screenshot shows the AWS EC2 'Launch an instance' progress bar. It indicates that the 'Creating security group rules' step is currently in progress, at 23% completion. The progress bar is blue with white text and a percentage indicator.

Details

Please wait while we launch your instance.
Do not close your browser while this is loading.



The screenshot shows the AWS EC2 'Launch an instance' success message. It displays a green notification bar stating 'Success' and 'Successfully initiated launch of instance (i-01af9fd5706f2e65e)'. Below this, there is a 'Launch log' section and a 'Next Steps' section with various options like 'Create billing usage alerts', 'Connect to your instance', 'Connect an RDS database', and 'Create EBS snapshot policy'.

CloudShell Feedback Console Mobile App

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Launch an instance | EC2 | eu-west-1 | + eu-west-1.console.aws.amazon.com/ec2/home?region=eu-west-1#LaunchInstances: Account ID: 3850-9853-8236 Europe (Ireland) breniesekar01

EC2 > Instances > Launch an instance

Success Successfully initiated launch of instance (i-01af9fd5706f2e65e)

Launch log

Next Steps

What would you like to do next with this instance, for example "create alarm" or "create backup".

1 2 3 4 5 6

Create billing usage alerts To manage costs and avoid surprise bills, set up email notifications for billing usage thresholds. Create billing alerts

Connect to your instance Once your instance is running, log into it from your local computer. Connect to instance Learn more

Connect an RDS database Configure the connection between an EC2 instance and a database to allow traffic flow between them. Connect an RDS database Create a new RDS database Learn more

Create EBS snapshot policy Create a policy that automates the creation, retention, and deletion of EBS snapshots. Create EBS snapshot policy

Manage detailed monitoring Create Load Balancer Create AWS budget Manage CloudWatch alarms

CloudShell Feedback Console Mobile App

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the AWS EC2 Instances page in a browser. The left sidebar is collapsed. The main area displays a table of instances. One instance, named "winServer01" with ID "i-01af9fd5706f2e65e", is listed as "Running". The table includes columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IPv4. The Public IPv4 column shows "ec2-54-74-2".

The screenshot shows the AWS EC2 Instances page with the instance "winServer01" selected. The left sidebar is collapsed. The main area shows detailed information for the selected instance. Under "Availability zone ID", it shows "euw1-az2". Under "IP addresses", it shows "Public IPv4 address: 54.74.240.50" and "Private IPv4 address: 172.31.31.169". There are also sections for "Secondary private IPv4 addresses" and "Carrier IP addresses (ephemeral)".

The public IPv4 address **54.74.240.50** was noted, as it will be used to connect to the server through RDP.

Step 3: Connect using RDP and fetch the system information

3.1 : Connected using RDP (Pre-available in windows)

Get Login Credentials

In the EC2 console, the instance was selected and the option Actions → Security → Get Windows password was used. The .pem key file was uploaded and decrypted, after which the username (Administrator) and password were obtained.

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with options like Dashboard, EC2 Global View, Events, Instances (selected), Images, and Elastic Block Store. The main area displays a table titled 'Instances (1/1) Info' with one row for 'winServer01'. The instance details include its ID (i-01af9fd5706f2e65e), state (Running), and type (t3.small). To the right of the table is a vertical Actions menu with options like 'Change security groups', 'Get Windows password', and 'Modify IAM role'. Below the table, there's a section for 'IP addresses Info' showing a Public IPv4 address (54.74.240.50) and a Private IPv4 address (172.31.31.169).

The screenshot shows the 'Get Windows password' dialog box. It starts with a note: 'Use your private key to retrieve and decrypt the initial Windows administrator password for this instance.' It lists the Instance ID (i-01af9fd5706f2e65e (winServer01)) and the Key pair associated with this instance (aws-ireland-win-key-pair). There's a 'Private key' section with a note: 'Either upload your private key file or copy and paste its contents into the field below.' A blue button labeled 'Upload private key file' is visible. Below it is a text input field labeled 'Private key contents' containing placeholder text: 'Private key contents'. At the bottom right are 'Cancel' and 'Decrypt password' buttons.

Get windows password | EC2

eu-west-1.console.aws.amazon.com/ec2/home?region=eu-west-1#GetWindowsPassword:instanceId=i-01af9fd5706f2e65e

aws Search [Alt+S]

EC2 Instances i-01af9fd5706f2e65e

Get Windows password

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

Instance ID: i-01af9fd5706f2e65e (winServer01)

Key pair associated with this instance: aws-ireland-win-key-pair

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

Upload private key file

Private key contents:

File name: aws-ireland-win-key-pair.pem

Open Cancel

Cancel Decrypt password

CloudShell Feedback Console Mobile App

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Get windows password | EC2

eu-west-1.console.aws.amazon.com/ec2/home?region=eu-west-1#GetWindowsPassword:instanceId=i-01af9fd5706f2e65e

aws Search [Alt+S]

EC2 Instances i-01af9fd5706f2e65e > Get Windows password

Get Windows password

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

Instance ID: i-01af9fd5706f2e65e (winServer01)

Key pair associated with this instance: aws-ireland-win-key-pair

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

Upload private key file

aws-ireland-win-key-pair.... X

1.67 KB

Private key contents:

```
-----BEGIN RSA PRIVATE KEY-----  
MIIEowIBAAQCAQEAvwyhhgB5j69view9zLrnW1neHbETwQ79PKrnCu6FxCAZLN2J+  
MXLvcOcmghB0d44Xrk8B2yEKWD2ZTNSo4M3ojwhzcif8ZhunJP+iwo3VwbunM  
wOVSTTU49oe5AKSxBzmhGpieZn2JK/w3f+nKtDgvSaZpg4brp4lOp8sM1B5G4+jp  
21SoCe55WM3Jey5632hEBBehU0+XqgTPfhugzYT1L1QkaT31v2FjfgX8qAsqAvfj  
+w0z91Mm7b80DAtwX6SNGNqdj33tSLW0SeRryN6e0cP9j3NqfVjEn5VfokuDsaTJ  
uyeq+hmU3NCmChcdxb+CwCTHO+Lvia3JBWx9QIDAQABaIBACQCO3HnRBbwgcLo  
ofzWasmyNHAcqJZuPh4r+Kvpz354r9QaQT+nstPfkWCKO5omljxe7/9fBQtRbj
```

CloudShell Feedback Console Mobile App

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

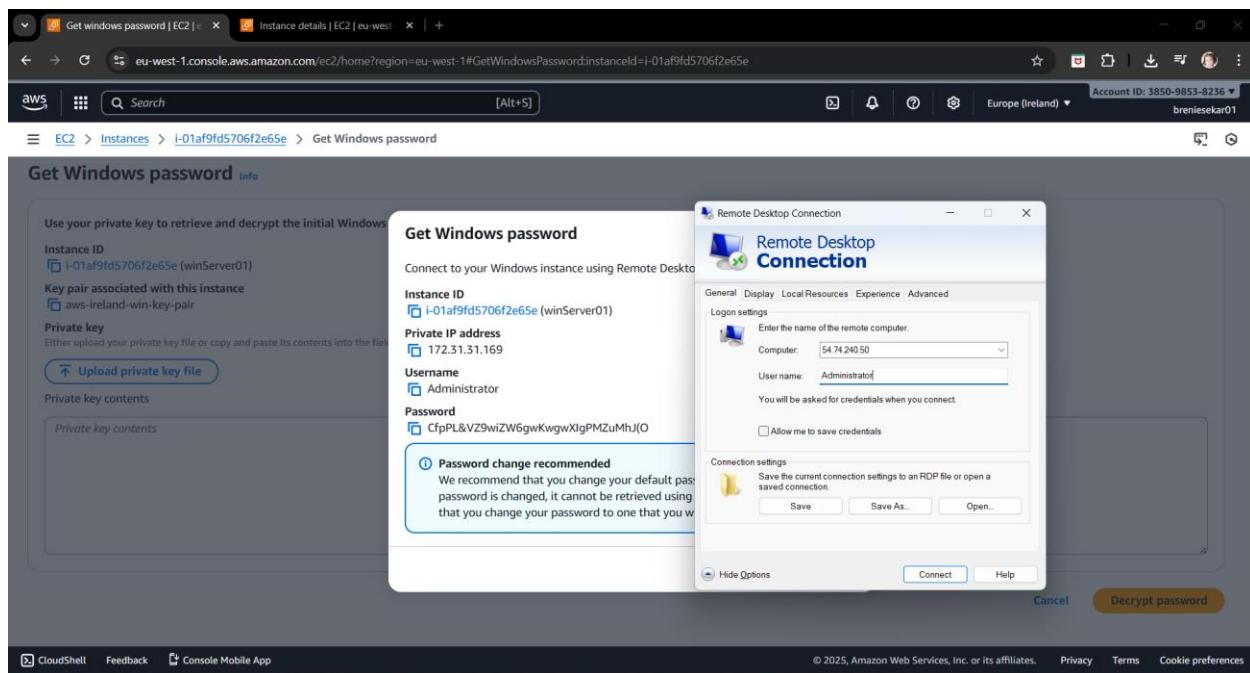
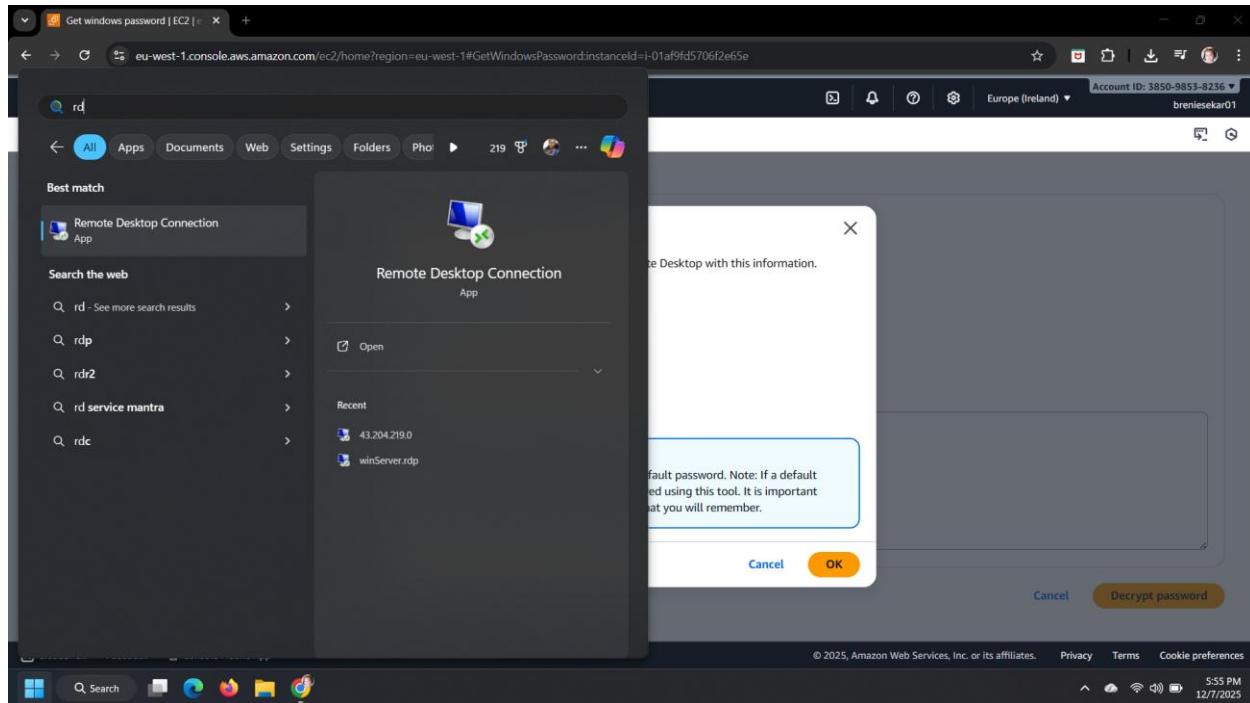
The screenshot shows the AWS CloudShell interface with the URL eu-west-1.console.aws.amazon.com/ec2/home?region=eu-west-1#GetWindowsPassword:instanceId=i-01af9fd5706f2e65e. The page displays the 'Get Windows password' step for an EC2 instance with Instance ID `i-01af9fd5706f2e65e` (winServer01). It shows the private key contents and a 'Decrypt password' button.

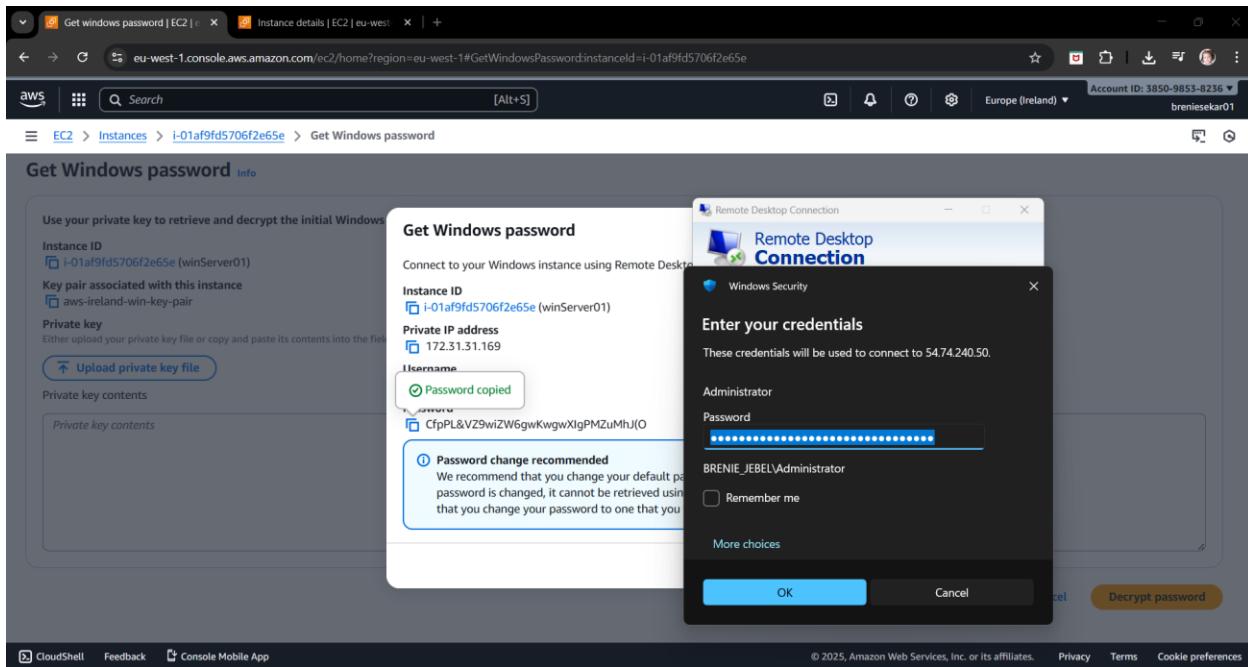
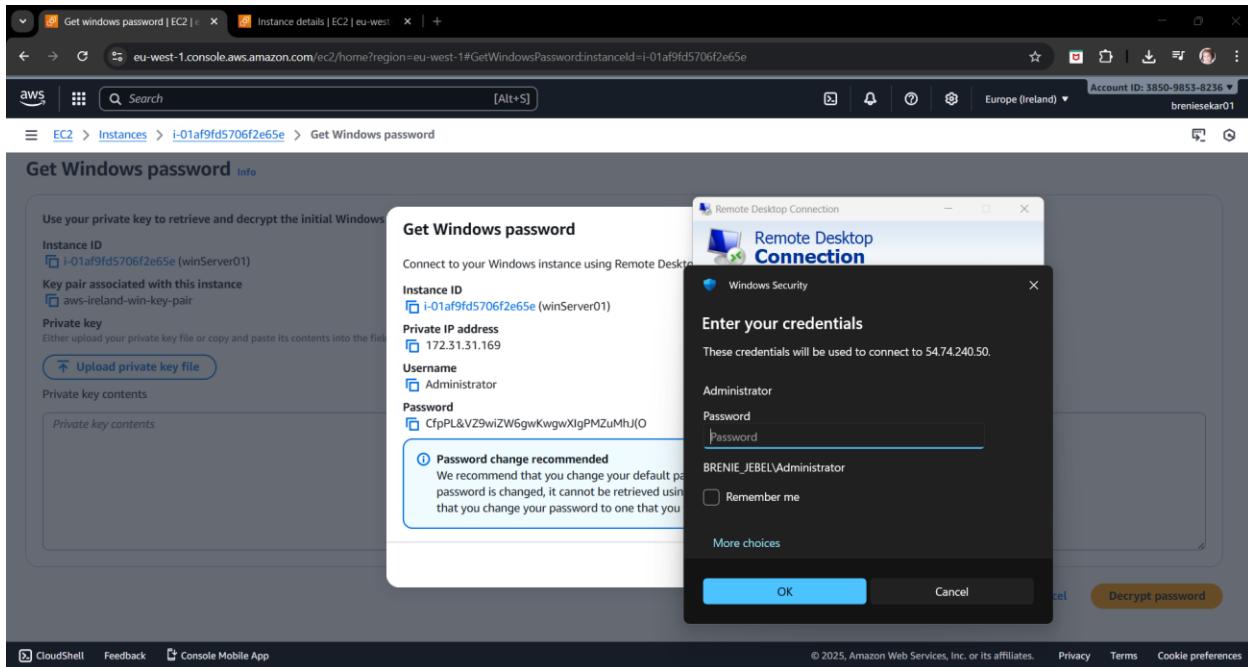
The screenshot shows the AWS CloudShell interface with the same URL as the previous screenshot. A modal dialog titled 'Get Windows password' is open, prompting the user to connect to the Windows instance using Remote Desktop. It displays the Instance ID `i-01af9fd5706f2e65e` (winServer01), Private IP address `172.31.31.169`, Username `Administrator`, and Password `CfpPL&V29wizW6gwKwgwXlgPMZuMhJ0`. A note at the bottom of the dialog recommends changing the password.

Open Remote Desktop

The Remote Desktop application was opened from the window search menu. In the RDP client, the public IP address of the instance was entered.

The connection was then established using the Administrator username and password.





The screenshot shows a browser window with two tabs: 'Get windows password | EC2' and 'Instance details | EC2 | eu-west-1'. The main content is the 'Get Windows password' page for instance 'i-01af9fd5706f2e65e (winServer01)'. It displays the instance ID, key pair, private IP address, and a 'Private key contents' section. A message box says 'Password copied'. In the background, a 'Remote Desktop Connection' window is open, showing a progress bar for connecting to '54.74.245.50'.

Get Windows password

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

Instance ID
i-01af9fd5706f2e65e (winServer01)

Key pair associated with this instance
aws-ireland-win-key-pair

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

Upload private key file

Private key contents

Get Windows password

Connect to your Windows instance using Remote Desktop.

Instance ID
i-01af9fd5706f2e65e (winServer01)

Private IP address
172.31.31.169

Username
CfpPL&VZ9wiZW6gwKwgwXlgPMZuMhj(O)

>Password change recommended
We recommend that you change your default password. If your password is changed, it cannot be retrieved using this method.

Remote Desktop Connection

Connecting to: 54.74.245.50

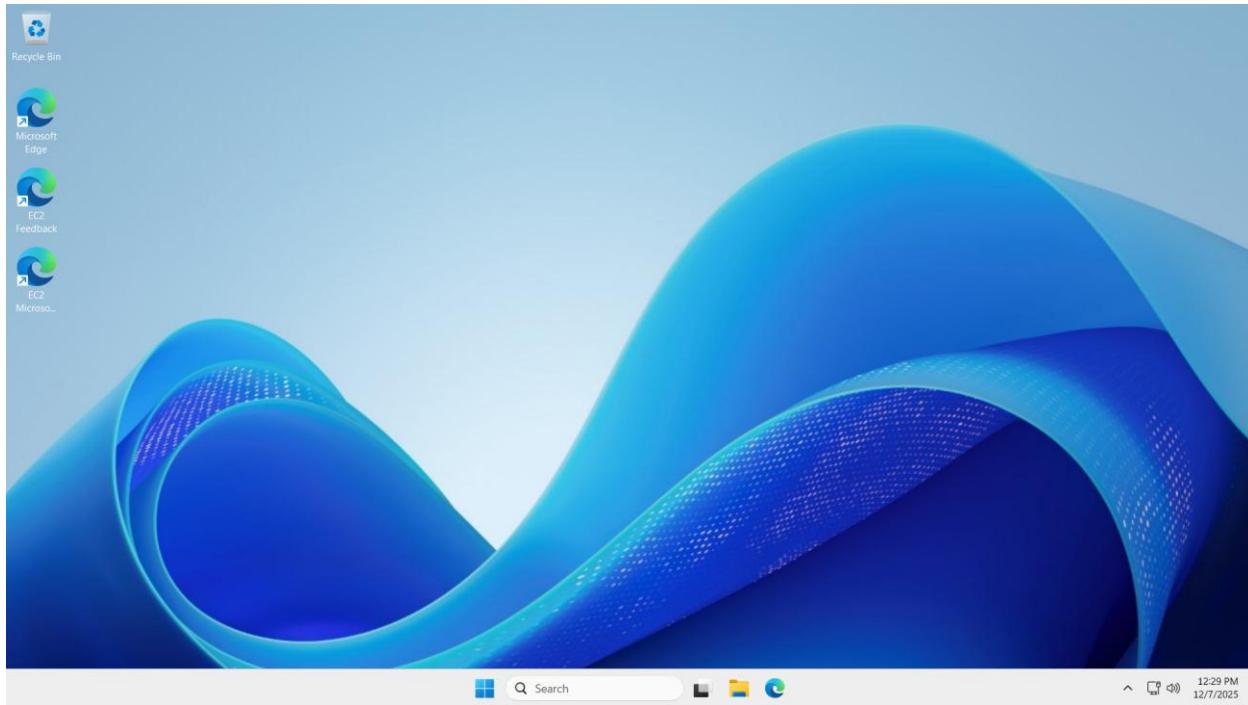
Configuring remote session...

Connection settings
Save the current connection settings to an RDP file or open a saved connection.

Save Save As... Open... Hide Options Connect Help

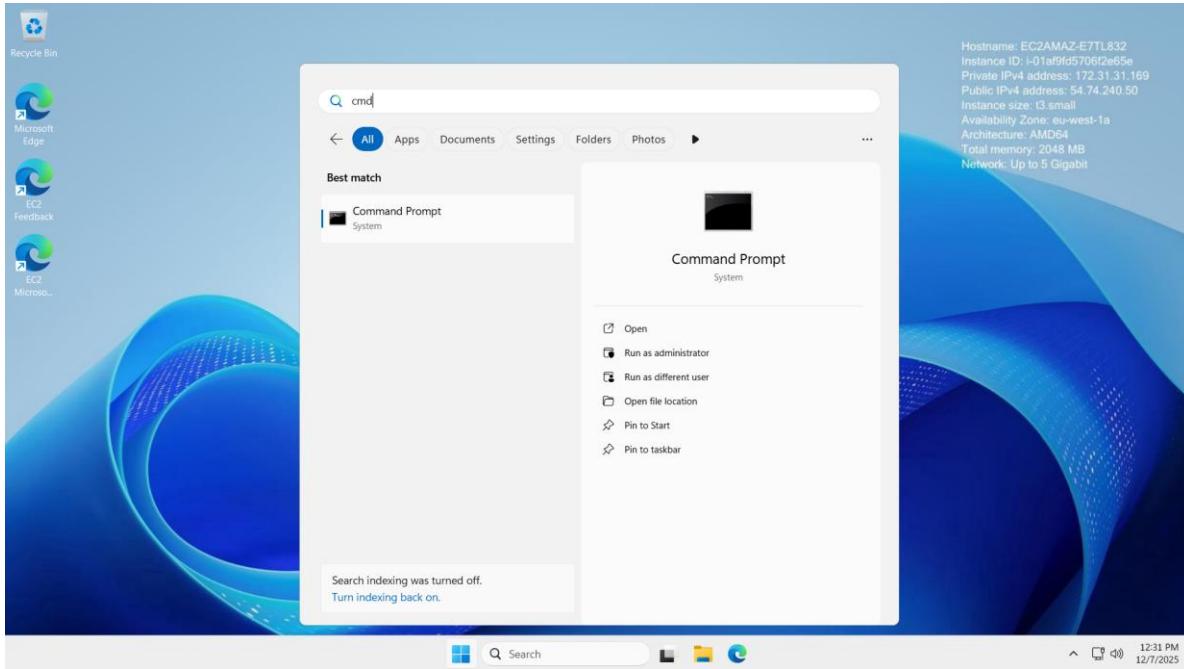
CloudShell Feedback Console Mobile App

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

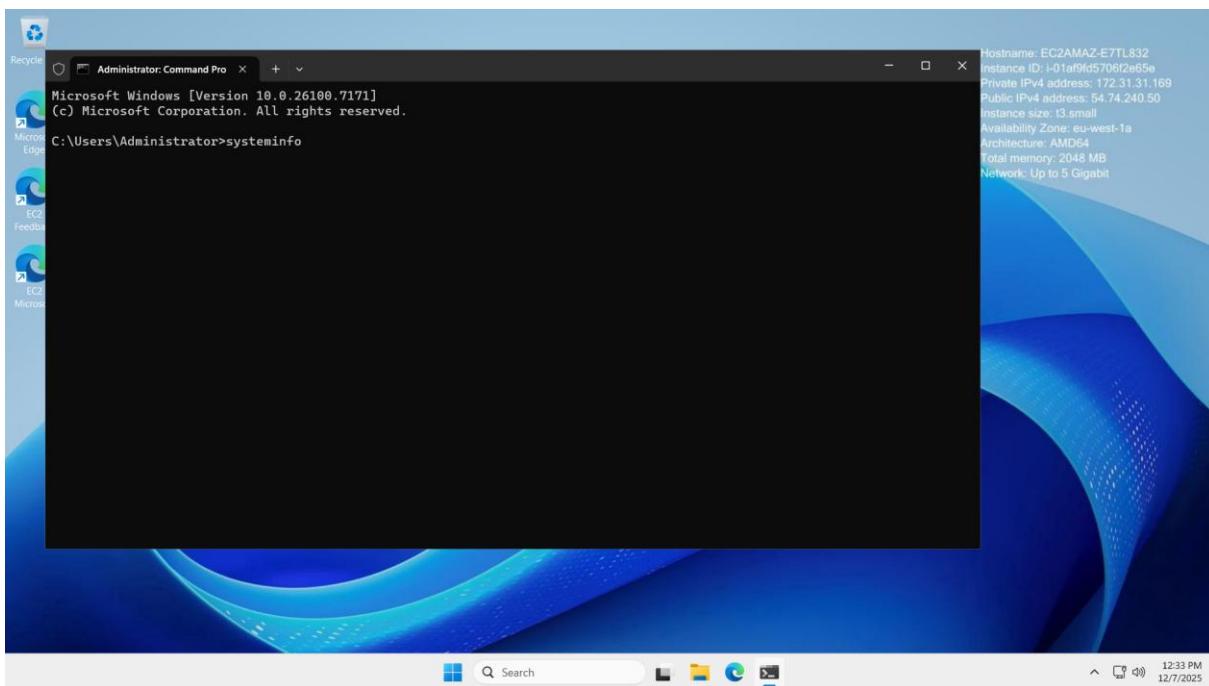


Check System Info

The Command Prompt was opened by pressing Win + R, typing cmd, and confirming with Enter.



Once the terminal was launched, the command “**systeminfo**” was executed to retrieve system details of the Windows virtual machine.



```
Administrator: Command Pro + 
Microsoft Windows [Version 10.0.26100.7171]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>systeminfo

Host Name: EC2AMAZ-E7TL832
OS Name: Microsoft Windows Server 2025 Datacenter
OS Version: 10.0.26100 N/A Build 26100
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Server
OS Build Type: Multiprocessor Free
Registered Owner: EC2
Registered Organization: Amazon.com
Product ID: 00491-50000-00001-AA661
Original Install Date: 12/6/2025, 5:49:46 PM
System Boot Time: 12/7/2025, 12:19:54 PM
System Manufacturer: Amazon EC2
System Model: t3.small
System Type: x64-based PC
Processor(s):
  1 Processor(s) Installed.
    [01]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel ~2500 Mhz
    Amazon EC2 1.0, 10/16/2017
BIOS Version: Windows Directory: C:\Windows
System Directory: C:\Windows\system32
Boot Device: \Device\HarddiskVolume2
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (UTC) Coordinated Universal Time
Total Physical Memory: 1,894 MB
Available Physical Memory: 397 MB

Hostname: EC2AMAZ-E7TL832
Instance ID: i-01af905706f2e65e
Private IPv4 address: 172.31.31.169
Public IPv4 address: 54.74.240.50
Instance size: t3.small
Availability Zone: eu-west-1a
Architecture: AMD64
Total memory: 2048 MB
Network: Up to 5 Gigabit

12:35 PM 12/7/2025
```

```
Administrator: Command Pro + 
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (UTC) Coordinated Universal Time
Total Physical Memory: 1,894 MB
Available Physical Memory: 397 MB
Virtual Memory: Max Size: 3,016 MB
Virtual Memory: Available: 1,321 MB
Virtual Memory: In Use: 1,725 MB
Page File Location(s): C:\pagefile.sys
Domain: WORKGROUP
Logon Server: \\EC2AMAZ-E7TL832
Hotfix(s):
  3 Hotfix(s) Installed.
    [01]: KB5066131
    [02]: KB5068861
    [03]: KB5067035
Network Card(s):
  1 NIC(s) Installed.
    [01]: Amazon Elastic Network Adapter
      Connection Name: Ethernet
      DHCP Enabled: Yes
      DHCP Server: 172.31.16.1
      IP address(es)
        [01]: 172.31.31.169
        [02]: fe80::db7f:bf1f:7d2:9610
Virtualization-based security: Status: Not enabled
  App Control for Business policy: Enforced
  App Control for Business user mode policy: Off
  Security Features Enabled:
Hyper-V Requirements: A hypervisor has been detected. Features required for Hyper-V will not be displayed.

C:\Users\Administrator>
```

The output details of the system configuration and environment were then captured and shared below :

C:\Users\Administrator>systeminfo

Host Name: EC2AMAZ-E7TL832
OS Name: Microsoft Windows Server 2025 Datacenter
OS Version: 10.0.26100 N/A Build 26100
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Server
OS Build Type: Multiprocessor Free
Registered Owner: EC2
Registered Organization: Amazon.com
Product ID: 00491-50000-00001-AA661
Original Install Date: 12/6/2025, 5:49:46 PM
System Boot Time: 12/7/2025, 12:19:54 PM
System Manufacturer: Amazon EC2
System Model: t3.small
System Type: x64-based PC
Processor(s): 1 Processor(s) Installed.
[01]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel ~2500 Mhz
BIOS Version: Amazon EC2 1.0, 10/16/2017
Windows Directory: C:\Windows
System Directory: C:\Windows\system32
Boot Device: \Device\HarddiskVolume2
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (UTC) Coordinated Universal Time
Total Physical Memory: 1,894 MB
Available Physical Memory: 397 MB
Virtual Memory: Max Size: 3,046 MB
Virtual Memory: Available: 1,321 MB
Virtual Memory: In Use: 1,725 MB
Page File Location(s): C:\pagefile.sys
Domain: WORKGROUP
Logon Server: \\EC2AMAZ-E7TL832
Hotfix(s): 3 Hotfix(s) Installed.
[01]: KB5066131
[02]: KB5068861
[03]: KB5067035
Network Card(s): 1 NIC(s) Installed.
[01]: Amazon Elastic Network Adapter
Connection Name: Ethernet
DHCP Enabled: Yes
DHCP Server: 172.31.16.1
IP address(es)
[01]: 172.31.31.169
[02]: fe80::db7f:bf1f:7d2:9610

Virtualization-based security: Status: Not enabled

App Control for Business policy: Enforced

App Control for Business user mode policy: Off

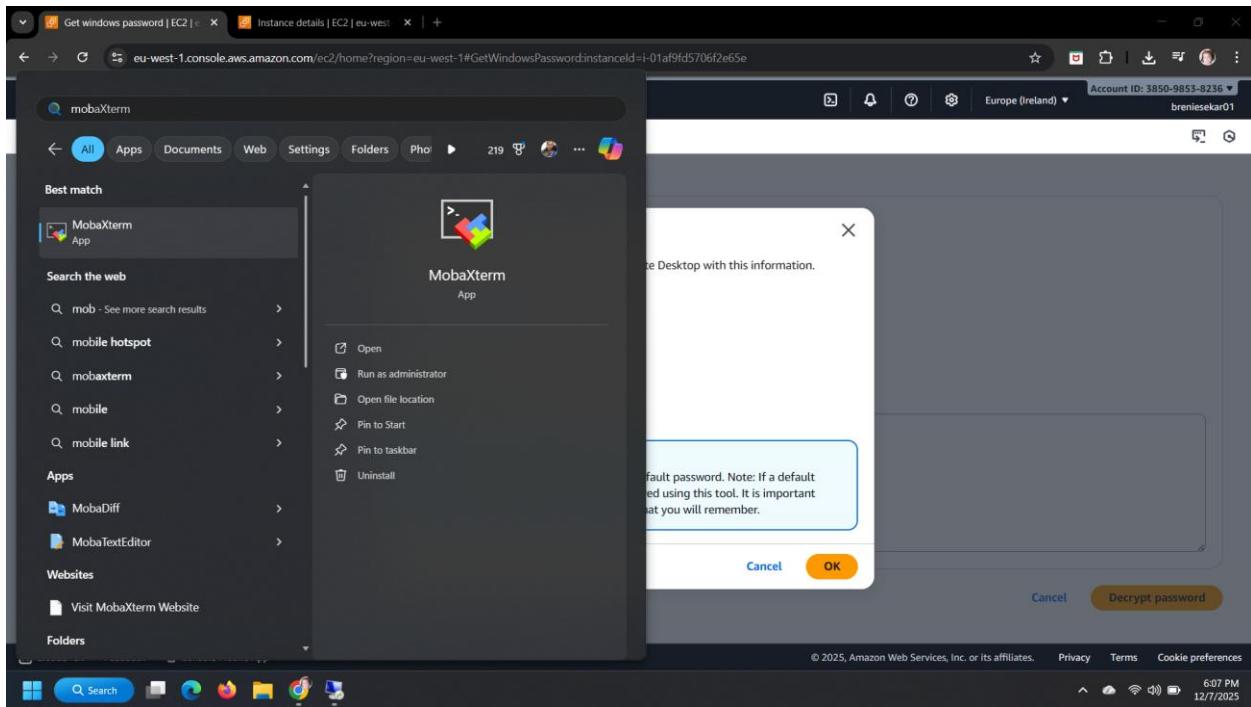
Security Features Enabled:

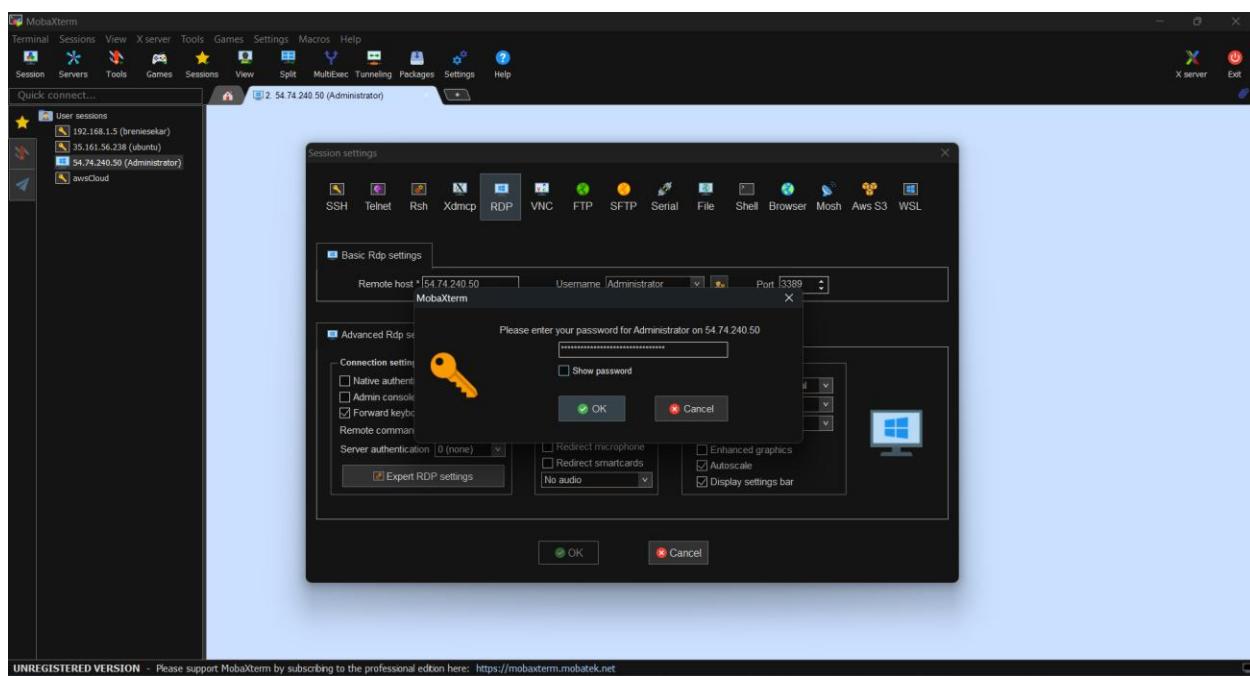
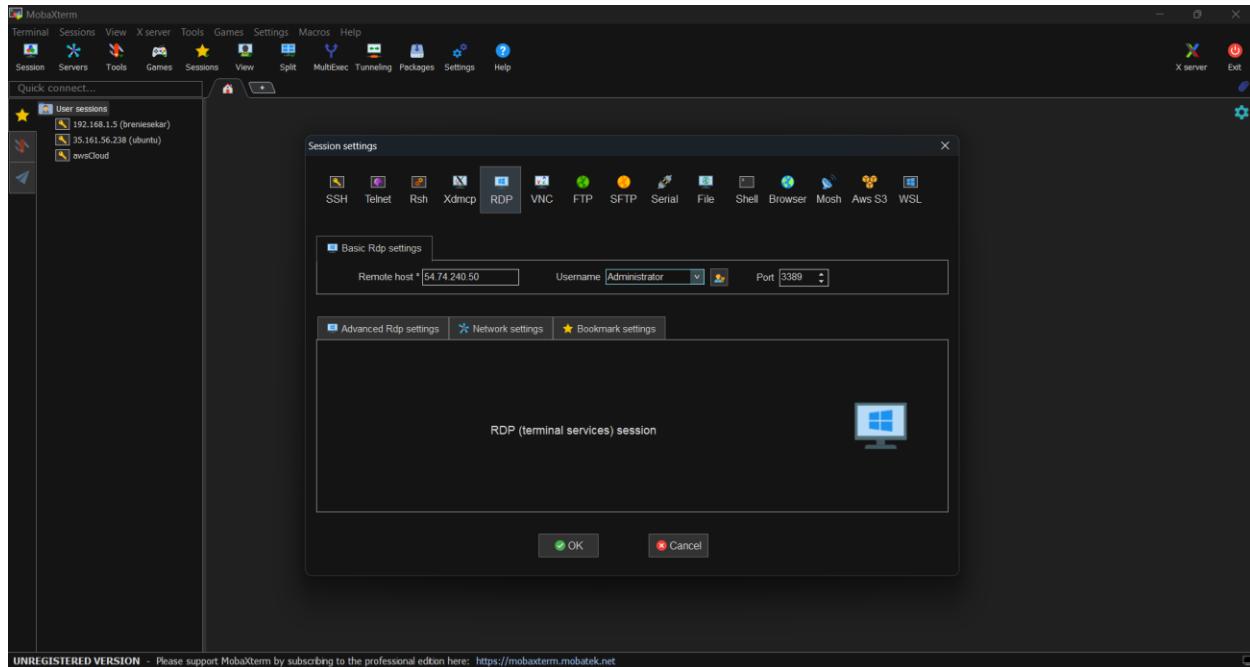
Hyper-V Requirements: A hypervisor has been detected. Features required for Hyper-V will not be displayed.

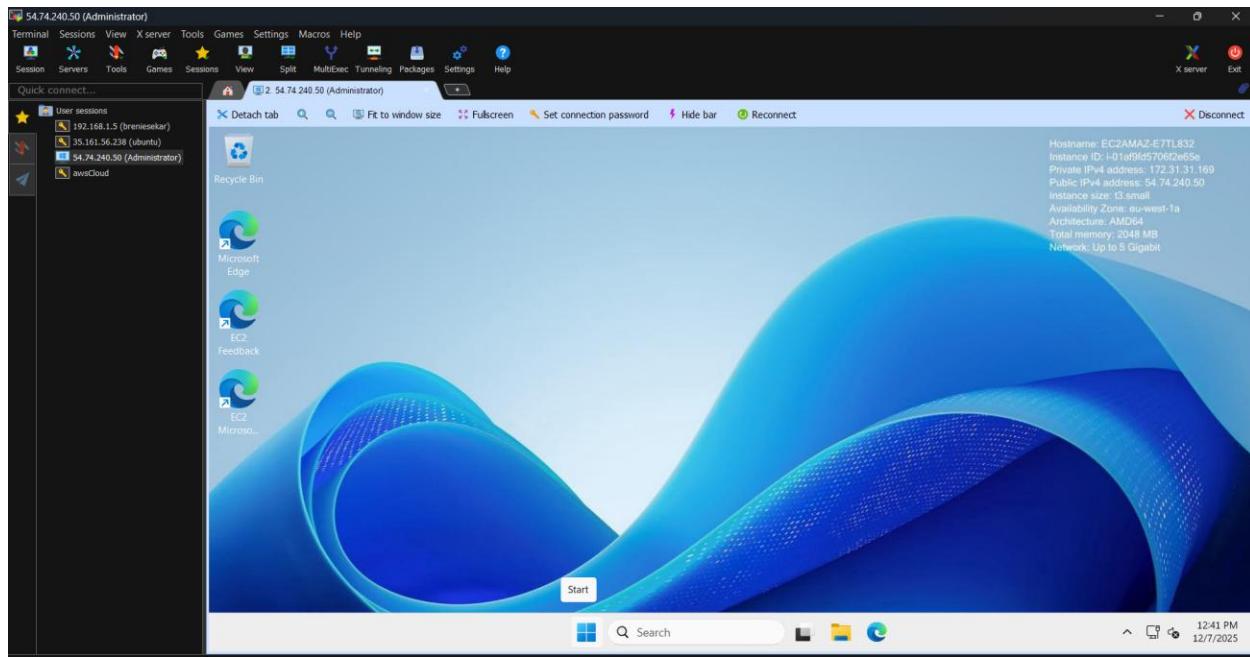
3.2 : Connected using MobaXterm

Open MobaXterm → Session

MobaXterm was opened and a new session was created. The RDP session type was selected, and the public IP address of the instance was entered as the remote host. The username Administrator and the decrypted password obtained from AWS were provided. The connection was established by selecting OK.

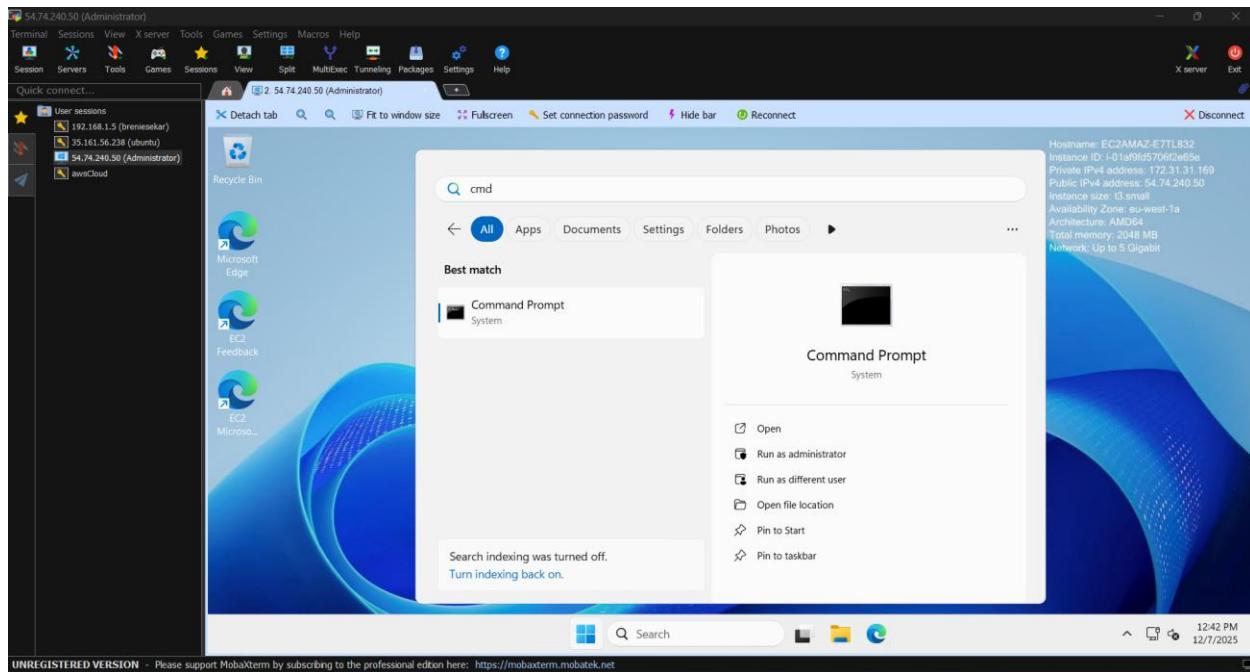


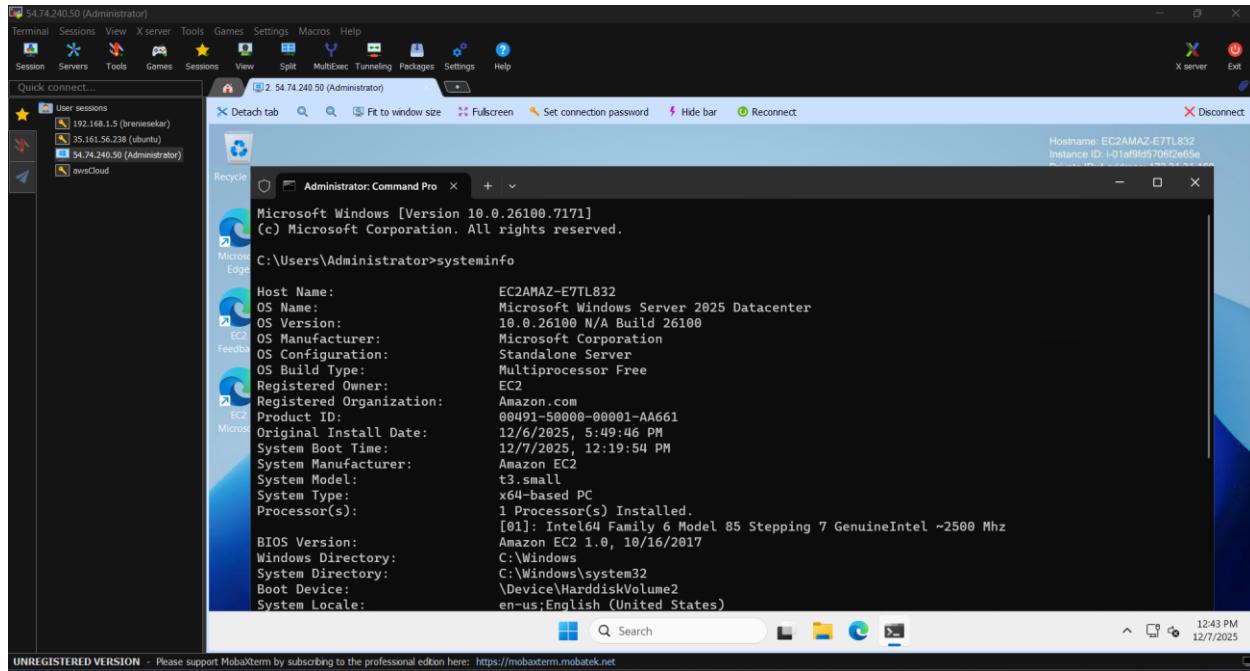




Open CMD inside Windows

After the RDP connection was established, the Command Prompt within the Windows environment was opened. The command “**systeminfo**” was executed to display the system information of the virtual machine.





Step 4: Clean up

4.1 : Delete the created instance

In the EC2 console, the instance “winServer01” was selected. The option Instance State → Terminate was used, and the termination was confirmed. The instance stopped and was removed from the list shortly afterwards.

Instance ID	Name	Instance State	Instance Type	Status
i-01af9fd5706f2e65e	winServer01	Stopping	t3.small	-

Actions

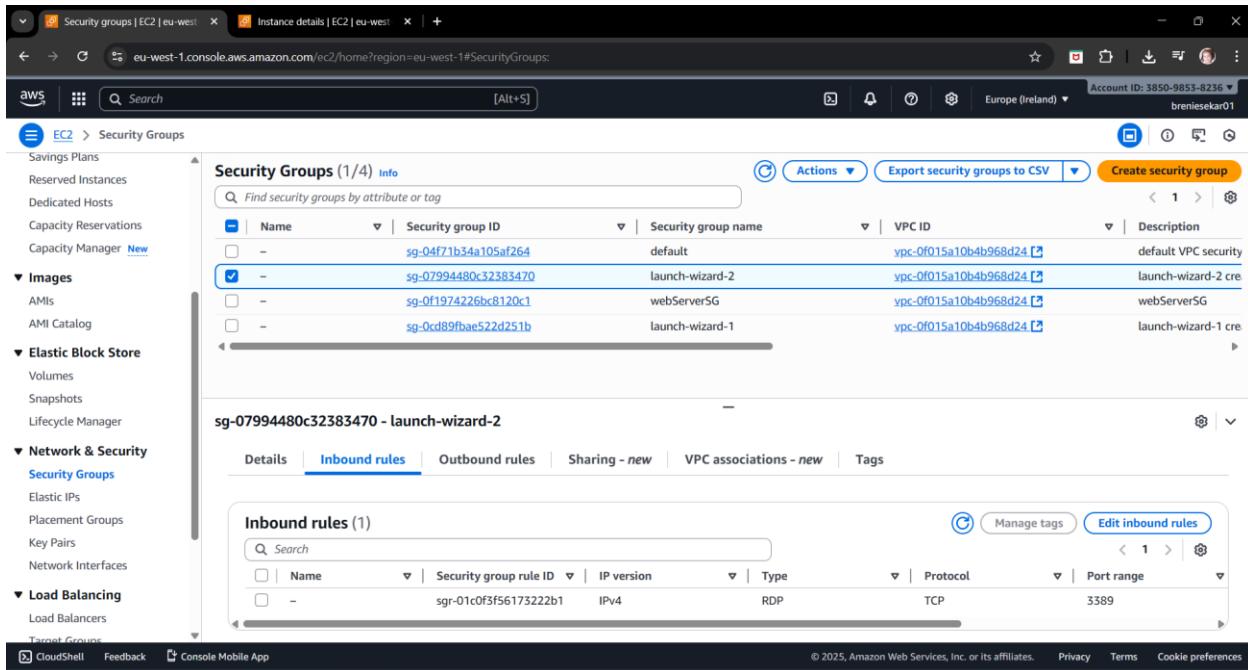
- Force stop instance
- Reboot instance
- Hibernate instance
- Terminate (delete) instance

The screenshot shows the AWS EC2 Instances page. A modal dialog titled "Terminate (delete) instance" is open. It contains a warning message: "On an EBS-backed instance, the default action is for the root EBS volume to be deleted when the instance is terminated. Storage on any local drives will be lost." Below this, a confirmation message asks, "Are you sure you want to terminate these instances?" There are two options: "Instance ID" (checkbox checked) and "Termination protection" (radio button selected). The "Termination protection" option is described as "Disabled". Below the checkboxes, there is a note: "To confirm that you want to delete the instances, choose the terminate button below. Instances with termination protection enabled will not be terminated. Terminating the instance cannot be undone." At the bottom of the modal are "Cancel" and "Terminate (delete)" buttons.

The screenshot shows the AWS EC2 Instances page after the instance has been terminated. A green success message at the top states "Successfully initiated termination (deletion) of i-01af9fd5706f2e65e". The main table shows the instance status as "Terminated". The instance details page for "i-01af9fd5706f2e65e (winServer01)" is displayed, showing the "terminated" state in the "Instance state" column. The "Actions" dropdown menu is open, showing options like "Launch instances", "Stop", "Start", "Reboot", "Replace", "Delete", and "View alarms".

4.2 : Delete the created security group

After the instance was terminated, the created security group “launch-wizard-2” was deleted. In the EC2 console, the Security Groups section was opened, and the created security group was selected. The option Actions → Delete Security Group was chosen, and the deletion was confirmed.

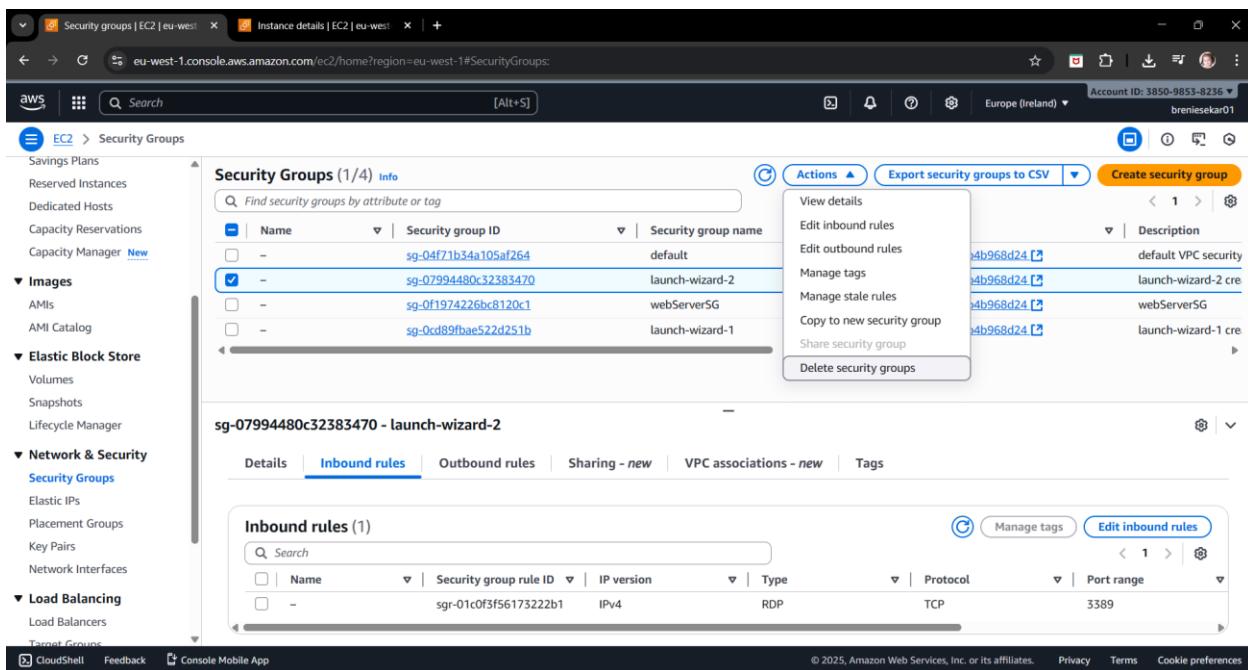


The screenshot shows the AWS EC2 Security Groups page. On the left, there's a navigation sidebar with options like Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Capacity Manager, Images, AMIs, AMI Catalog, Elastic Block Store, Volumes, Snapshots, Lifecycle Manager, Network & Security (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), Load Balancing (Load Balancers), and Transit Groups. The main area displays a table of security groups:

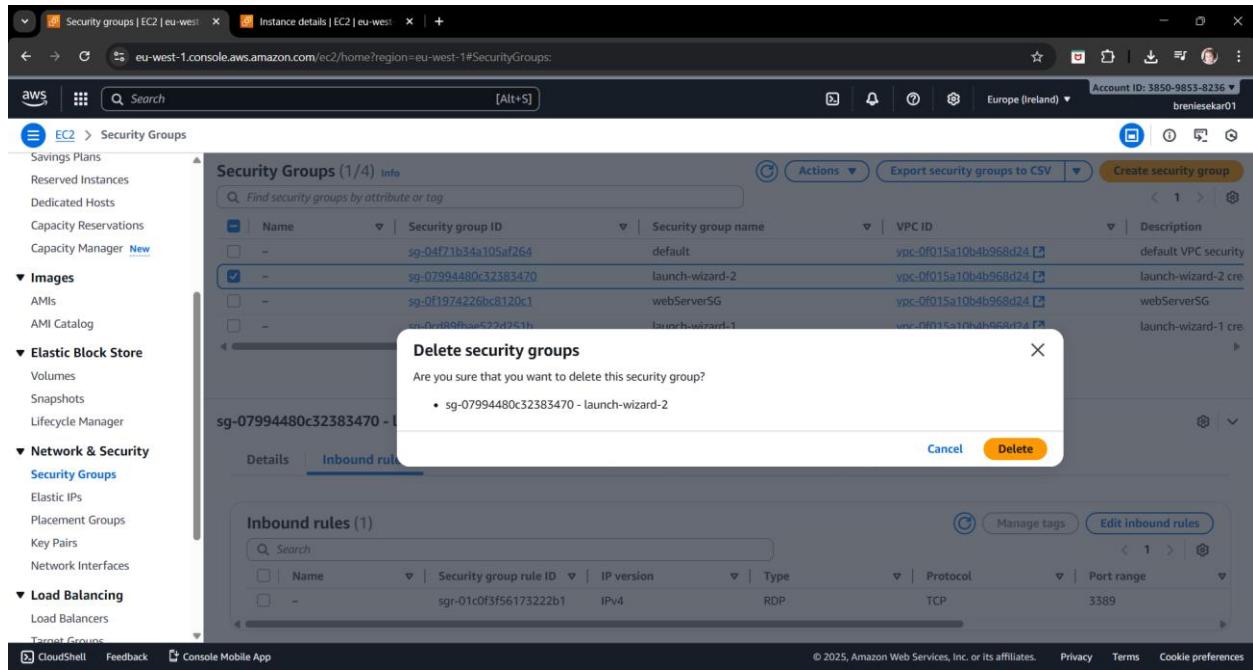
Name	Security group ID	Security group name	VPC ID	Description
-	sg-04f71b34a105af264	default	vpc-0f015a10b4b968d24	default VPC security
<input checked="" type="checkbox"/>	sg-07994480c32383470	launch-wizard-2	vpc-0f015a10b4b968d24	launch-wizard-2 cre
-	sg-0f1974226be8120c1	webServerSG	vpc-0f015a10b4b968d24	webServerSG
-	sg-0cd89fbbae522d251b	launch-wizard-1	vpc-0f015a10b4b968d24	launch-wizard-1 cre

Below the table, a modal window for the selected security group "sg-07994480c32383470 - launch-wizard-2" is open. It shows the Inbound rules tab, which lists one rule:

Name	Security group rule ID	IP version	Type	Protocol	Port range
-	sgr-01c0f3f56173222b1	IPv4	RDP	TCP	3389



This screenshot is identical to the one above, showing the AWS EC2 Security Groups page. The "Actions" dropdown menu is open over the selected security group "sg-07994480c32383470 - launch-wizard-2". The "Delete security groups" option is highlighted with a red box. Other options in the menu include View details, Edit inbound rules, Edit outbound rules, Manage tags, Manage stale rules, Copy to new security group, Share security group, and View details again.



Task Summary :

- Logged in to the AWS Management Console.
- Created a Windows EC2 virtual machine using the Windows Server AMI.
- Configured the instance with a key pair and security group allowing RDP access.
- Connected to the Windows VM:
 - Using the default Remote Desktop application.
 - Using MobaXterm.
- Opened Command Prompt inside the VM and executed systeminfo to verify system details.
- Performed cleanup:
 - Terminated the created EC2 instance.
 - Deleted the associated security group.