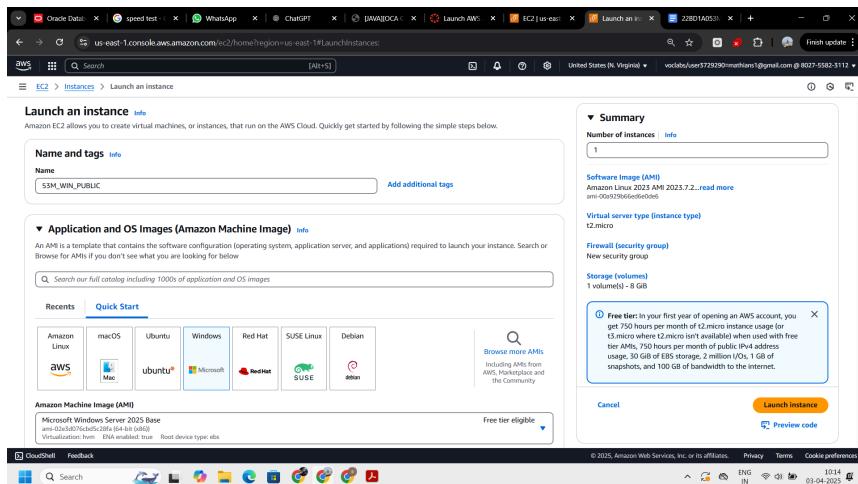


VPC CONNECTING PRIVATE TO INTERNET WINDOWS AMI

we created a **VPC (Virtual Private Cloud)** with an **IPv4 CIDR of 10.0.0.0/16**, We then created two **subnets**—one **public** (10.0.1.0/24) and one **private** (10.0.2.0/24)—within the VPC. To enable internet access for the public subnet, we set up an **Internet Gateway (IGW)** and attached it to the VPC. Finally, we created a **Route Table**, linked it to the public subnet, and configured it to route external traffic via the Internet Gateway.

Now Create a public web server instance Give a name(web-server2), and choose WINDOWS for AMI, t3.micro as instance type, use pem keypair

In the Network click on edit, choose the vpc, and select the public subnet



Add security group rules

Set rdp to my ip

http->anywhere

https->anywhere

The screenshot shows the AWS EC2 Instances Launch screen. On the left, there's a sidebar with navigation links like 'CloudShell', 'Feedback', and a search bar. The main area is titled 'Launch an instance' and contains three sections for defining security group rules:

- Security group rule 1 (TCP, 3389, 185.62.112.229/32):** Type: rdp, Protocol: TCP, Port range: 3389, Source type: My IP, Name: e.g. SSH for admin desktop, Description: optional.
- Security group rule 2 (TCP, 80, 0.0.0.0/0):** Type: HTTP, Protocol: TCP, Port range: 80, Source type: Anywhere, Name: e.g. SSH for admin desktop, Description: optional.
- Security group rule 3 (TCP, 443, 0.0.0.0/0):** Type: HTTPS, Protocol: TCP, Port range: 443, Source type: Anywhere, Name: e.g. SSH for admin desktop, Description: optional.

To the right, a summary panel shows the instance configuration:

- Summary:** Number of instances: 1
- Software Image (AMI):** Microsoft Windows Server 2025 ...read more
- Virtual server type (instance type):** t3.micro
- Firewall (security group):** New security group
- Storage (volumes):** 1 volume(s) - 30 GiB

A callout box highlights the 'Free tier' information: 'In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs. 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GiB of bandwidth to the internet.'

At the bottom right are 'Cancel', 'Launch Instance', and 'Preview code' buttons.

CREATE A NEW INSTANCE CALLED PRIVATE INSTANCE AND CHOOSE WINDOWS Type is t3 micro

The screenshot shows the AWS EC2 Instances Launch screen. The interface is similar to the previous one, with a sidebar and a main configuration area. In the main area, the 'Name and tags' section has '53M_WIN_PRIVATE' entered. The 'Application and OS Images (Amazon Machine Image)' section shows a search bar and a grid of recent AMI icons for Amazon Linux, macOS, Ubuntu, Windows, Red Hat, SUSE Linux, and Debian. Below this is the 'Amazon Machine Image (AMI)' details for 'Microsoft Windows Server 2025 Base': ami-02e5d076cbd5c28fa (64-bit (x86_64)), Virtualization: hvm, ENA enabled: true, Root device type: ebs, and a note that it's 'Free tier eligible'.

The summary panel on the right shows the configuration again, including the 'Free tier' information about 750 hours of t2.micro usage per month.

At the bottom right are 'Cancel', 'Launch Instance', and 'Preview code' buttons.

Choose rdp in security groups and then choose custom there enter the private ip address from the public instance

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

Security group name - required
launch-wizard-8

Description - required | Info
launch-wizard-8 created 2025-04-03T04:52:00.606Z

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 3389, 10.0.1.80)

Type Info	Protocol Info	Port range Info
rdp	TCP	3389
Source type Info	Source Info	Description - optional Info
Custom	<input type="text"/> Add CIDR, prefix list or security group	e.g. SSH for admin desktop
10.0.1.80		

Add security group rule Advanced network configuration

Summary

Number of instances | Info
1

Software Image (AMI)
Microsoft Windows Server 2025 ...read more
ami-02e3d076cb5c28fa

Virtual server type (instance type)
t3.micro

Firewall (security group)
New security group

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

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GiB of bandwidth to the internet.

Cancel Launch instance Preview code

Connect the public instance using the details given

EC2 > Instances > i-05e4d3fa0c35d6587 > Connect to instance

Connect to instance | Info
Connect to your instance i-05e4d3fa0c35d6587 (53M_WIN_PUBLIC) using any of these options:

- Session Manager
- RDP client
- EC2 serial console

Instance ID: i-05e4d3fa0c35d6587 (53M_WIN_PUBLIC)

Connection Type:
 Connect using RDP client
 Download a file to use with your RDP client and retrieve your password.

You can connect to your Windows instance using a remote desktop client of your choice, or download the remote desktop file.

[Download remote desktop file](#)

When prompted, connect to your instance using the following username and password:

Public IP: 100.27.20.236
 Password copied
 If you've joined your instance to a directory, you can use your directory credentials

Remote Desktop Connection

Computer: 100.27.20.236
 User name: None specified
 You will be asked for credentials when you connect.
[Show Options](#) [Connect](#) [Help](#)

Windows Security

To connect to the instance using Fleet Remote Desktop, the SSM Agent must be installed and running on the instance. For Agent

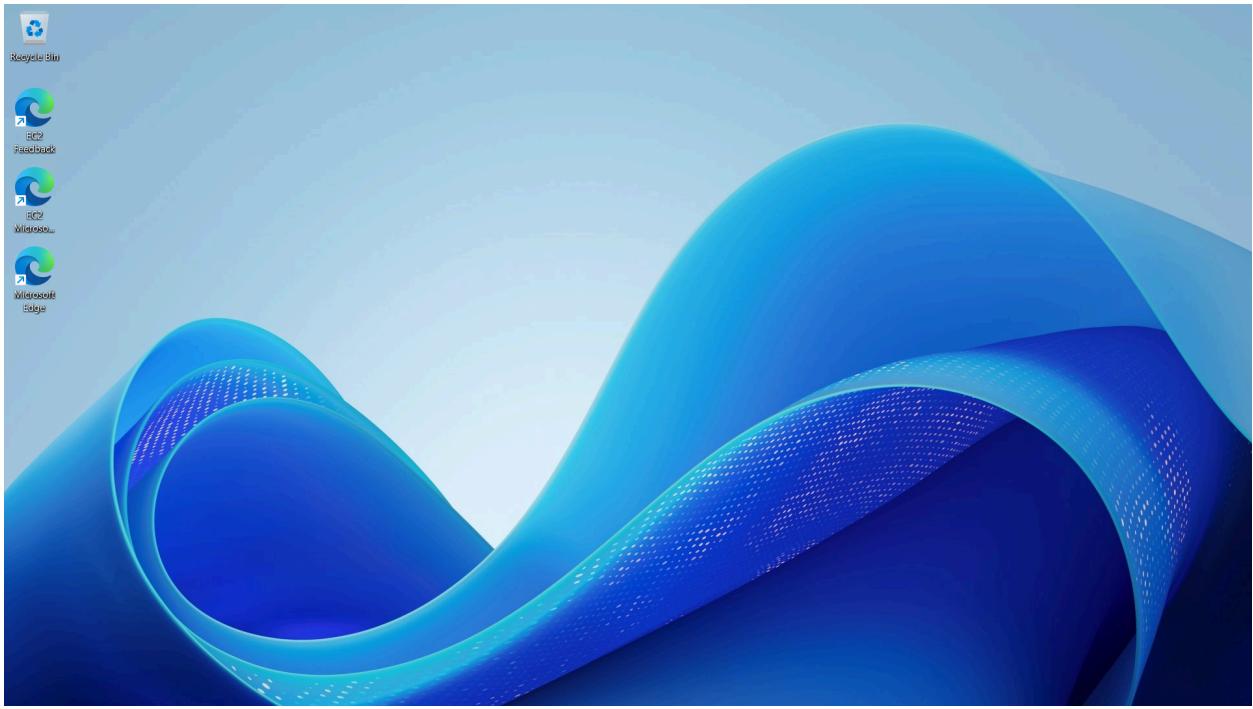
Enter your credentials

These credentials will be used to connect to 100.27.20.236.

User name: Administrator
 Password:
 Remember me
[OK](#) [Cancel](#)

Cancel

SUCCESSFULLY CONNECTED TO THE PUBLIC instance

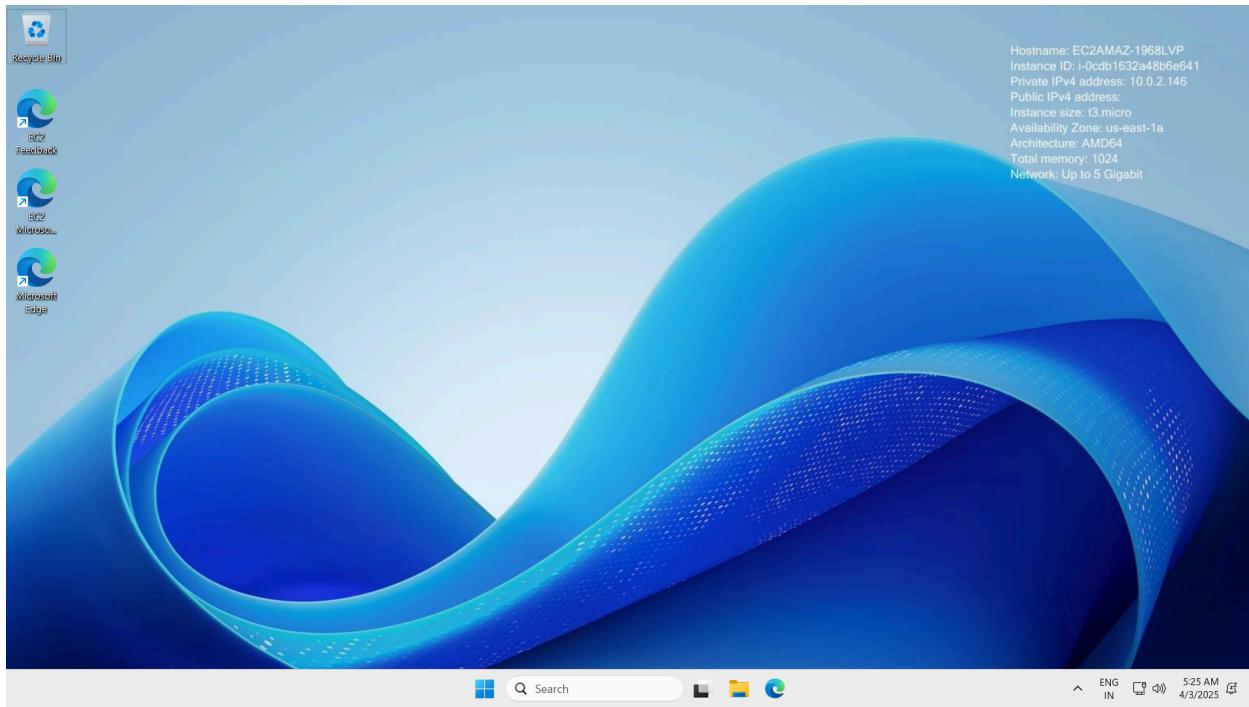


Now connect to the private instance

The screenshot shows the AWS EC2 Connect to instance page for an instance with ID i-0cdb1632a48b6e641. The page includes:

- A navigation bar at the top with tabs for Oracle Database, speed test, (80) What's New, ChatGPT, Java, Launch AMI, Instance details, Connect to instance, Untitled document, and 22BD1A05.
- A search bar and a dropdown for United States (N. Virginia).
- An instance ID selector showing i-0cdb1632a48b6e641 (53M_WIN_PRIVATE).
- A "Connect to instance" section with three tabs: Session Manager, RDP client (selected), and EC2 serial console.
- An "Instance ID" field containing i-0cdb1632a48b6e641 (53M_WIN_PRIVATE).
- A "Connection Type" section with two options:
 - Connect using RDP client: A note says "Download a file to use with your RDP client and retrieve your password."
 - Connect using Fleet Manager: A note says "To connect to the instance using Fleet Manager Remote Desktop, the SSM Agent must be installed and running on the instance. For more information, see Working with SSM Agent."
- A note below stating "You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below."
- A "Download remote desktop file" button.
- User authentication fields for "Private IP" (10.0.2.146) and "Username" (Administrator).
- A "Password" field with a "Get password" link.
- A note at the bottom: "If you've joined your instance to a directory, you can use your directory credentials to connect to your instance."
- A "Cancel" button in the bottom right corner.
- A footer with Cloudshell, Feedback, and various system status icons.

Connect to the private instance by opening rdp inside the public machine



Open cmd

Try a command like ping www.google.com

This show that the private system is also connected to the internet

