Ec2+puttygen

AWS is a cloud computing platform provided by Amazon. It offers a wide range of services you can access over the internet, like:

Storing data,Running applications, Hosting websites, Setting up virtual servers

Databases, AI tools, security services, etc.

You can rent what you need, use it, and pay for it based on your usage — instead of owning physical servers.

EC2 (Elastic Compute Cloud):

EC2 is one of the most popular services on AWS. It allows you to create virtual servers in the cloud called instances.

Instances = Virtual Machines (VMs) that you can run in the cloud.

------------------------------------------------------------------------------

What You Wanted to Do:

You wanted to create a virtual server (EC2 instance) on AWS and securely connect to it using from your Windows system using PuTTY and a converted private key. This is commonly done by system administrators and DevOps engineers for managing cloud infrastructure.

MobaXterm is a more powerful all-in-one terminal for Windows.

It includes an SSH client, SCP/SFTP file browser, X11 server (for GUIs), and multiple Unix commands pre-installed.t gives you a Linux-like experience on Windows.

What is PuTTY?  
PuTTY is a free and open-source SSH (Secure Shell) and telnet client. It lets you securely connect to remote servers (like your AWS EC2 instance). PuTTYgen is a companion tool used to convert key files (.pem to .ppk).

* PuTTY is a lightweight, free terminal emulator for Windows.
* It allows you to securely connect to remote servers using SSH, Telnet, SCP, etc.
* It comes with tools like PuTTYgen (for key conversion)
* Use it when you want You want a minimal, fast SSH client. You only need terminal access
* ------------------------------------------------------------------------------------------

Step 1: Launch an EC2 Instance

What you're doing: Creating a cloud-based virtual machine (Linux OS) on AWS.

How:

1. Sign in to AWS: <https://aws.amazon.com/>
2. Go to the EC2 Dashboard (search EC2 in top search bar).
3. Click “Launch Instance”.
4. Fill the following:

A. Name: “MyPuTTYInstance”

B. AMI: Amazon Linux 2 (or Ubuntu)

C. Instance Type: t2.micro (free tier eligible)

D. Key pair (Login):

* + Choose “Create new key pair”
  + Key pair name: “my-putty-key”
  + Key pair type: RSA
  + Private key format: .pem
  + Click “Create key pair” → it downloads a file like my-putty-key.pem

E. Network settings:

* + Edit → Check “Allow SSH traffic from anywhere” (port 22)

1. Click “Launch Instance”.

✅ Your EC2 instance is running. You now have a PEM file (key) used to authenticate your login.

-----------------------------------------------

Step 2: Download PuTTY Installer

1. Go to the official PuTTY website:  
   👉 https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html
2. Scroll down to the “Package files” section.
3. Choose the installer based on your Windows system:
   * For most users, download:  
     ✅ 64-bit: putty-64bit-<version>-installer.msi
4. Click to download the MSI file.

🔧 Step 3: Install PuTTY

1. Locate the downloaded file (in your Downloads folder):  
   e.g., putty-64bit-0.80-installer.msi
2. Double-click to open it.
3. The PuTTY Setup Wizard opens:
   * Click Next
   * Choose installation location (default is fine)
   * Click Install
   * Click Finish

🟢 PuTTY and PuTTYgen are now installed on your system.

🔧 Step 4: Open PuTTY or PuTTYgen

* Press the Windows key and search:
  + “PuTTY” — for SSH connections
  + “PuTTYgen” — to convert .pem keys to .ppk

Step 5: Convert PEM to PPK Using PuTTYGen

What you're doing: Converting your AWS PEM private key into a PPK file PuTTY can use.

Why? PuTTY (the Windows SSH client) doesn’t accept .pem files. It uses .ppk instead

How:

1. Open PuTTYGen (search “PuTTYGen” in Start menu)
2. In PuTTYGen:
   * Click “Load”
   * Change file type to “All Files (*.*)”
   * Select your .pem file (e.g., my-putty-key.pem)
3. Click “Save private key”
   * You can ignore the passphrase warning for now
   * Save as my-putty-key.ppk

✅ You now have a PuTTY-compatible private key (.ppk)

─────────────────────────────

🧩 Step 3: Get the Public IP of Your EC2 Instance

What you're doing: Getting the “address” of your cloud server.

How:

1. Go to EC2 Dashboard → Instances
2. Click your instance
3. Copy the Public IPv4 address (e.g., 3.80.202.45)

─────────────────────────────

🖥️ Step 4: Connect to EC2 Using PuTTY

What you're doing: Using PuTTY to SSH into your EC2 server using your PPK key.

How:

1. Open PuTTY (search “PuTTY” in Start menu)
2. In the “Host Name” field:
   * Enter: ec2-user@<your-public-ip> (e.g., ec2-user@3.80.202.45)
   * For Ubuntu, use ubuntu@ instead of ec2-user@
3. In the left sidebar:
   * Go to SSH → Auth
   * Click “Browse” and select your .ppk file (e.g., my-putty-key.ppk)
4. Click “Open”
   * If it’s your first time connecting, accept the security alert

✅ You are now connected to your EC2 instance via PuTTY

 You used an SSH key pair: AWS stores the public key, and you keep the private one.

 You used PuTTYGen to convert the private key into PPK format (which PuTTY can read).

 You used PuTTY (SSH client) to securely connect to your instance.

What You Can Do Now

Now that you’re logged into your EC2 instance using PuTTY, you can:

* Install software (Git, Python, Apache, etc.)
* Host a website or run apps
* Practice DevOps tools like Docker or Jenkins
* Set up a secure file server or testing environment