

2. EC2-Windows Launching

Launching EC2 Windows machine and verify it live – Step-by-Step (AWS Console)

Step 1: Login to AWS Console

- Open browser and go to <https://aws.amazon.com>
- Click on "Sign In to Console"
- Choose Root User and enter credentials

Step 2: Go to EC2 Dashboard

In the top search bar, type "EC2"

Click on "EC2" under "Services"

Click "Launch instance" button

Step 3: Configure EC2 Instance Basics

- Name: cst-R9ST-Windows-Instance
- Under "Application and OS Images (Amazon Machine Image)":
 - Choose: Microsoft Windows Server 2019 Base (Free tier eligible)
- Under "Instance type": Select **t2.micro** (Free tier eligible)
- Under "Key pair (login)":
 - If key pair exists, select it
 - If not, click "Create new key pair"
 - Name: cst-R9ST-Windows-Key
 - Key pair type: RSA
 - Private key file format: **.pem**
 - Click "Create key pair"
 - The **.pem** file will be downloaded automatically – save it safely
- Under "Network settings":

- Click "Edit"
- Auto-assign public IP: Enable
- Firewall: Allow RDP (port 3389)
 - Check the box: "Allow RDP traffic from"
 - Choose "Anywhere" (only for practice/demo)
- Storage:
 - Leave default 30 GiB General Purpose SSD (gp2) – Free tier eligible
- Click "Launch Instance"

Step 4: Wait for Instance to Launch

- Click "View All Instances"
- Wait until "Instance State" = "Running" and "Status Checks" = "2/2 checks passed"
- Note down the Public IPv4 address or Public DNS (Windows instance takes a few minutes to initialize)

Step 5: Connect to Windows EC2 via RDP

- Select the instance: cst-R9ST-Windows-Instance
- Click "Connect"
- Choose "RDP Client" tab
- Click "Download Remote Desktop File"
- Click "Get Password" (you may have to wait 4–5 minutes)
- Click "Choose File" and upload the .pem file that was downloaded earlier
- Click "Decrypt Password"
- Copy the "Username" (usually Administrator) and "Password"

Step 6: Launch the RDP File

- Open the .rdp file that was downloaded
- When prompted:

- Enter Username: Administrator
- Enter Password: (paste the decrypted password)
- Click "Yes" to any certificate warnings
- Wait for Windows desktop to appear – this confirms the EC2 is live and accessible

Step 7: Do a Quick Check Inside Windows EC2

- Once logged in, open Start Menu
- Click "This PC" to verify system
- Optionally, open browser (like IE/Edge) and go to <https://red9systech.com> (for demonstration)

Step 8: (Optional) Tag the Instance for Better Identification

- Go to EC2 > Instances
- Select the instance
- Click "Tags" tab > "Manage Tags"
- Add Tag:
 - Key: Project
 - Value: Red9SysTech-Batch1
- Save

Cleanup Steps – Delete Resources to Avoid Charges

Step 1: Stop and Terminate EC2 Instance

- Go to EC2 > Instances
- Select the instance: cst-R9ST-Windows-Instance
- Click "Instance state" > "Terminate instance"
- Confirm termination
- Wait until instance state shows "terminated"

Step 2: Delete Key Pair (optional)

- Go to EC2 Dashboard > Key Pairs
- Find and select **cst-R9ST-Windows-Key**
- Click "Actions" > "Delete"
- Confirm

Step 3: Delete Security Group (optional if created manually)

- Go to EC2 Dashboard > Security Groups
- Select the one associated with your instance (if custom created)
- Click "Actions" > "Delete security group"
- Confirm