| **Login Method** | **Description** | **Required Tools/Settings** | **Steps** |
| --- | --- | --- | --- |

|  |  |  |  |
| --- | --- | --- | --- |
| **SSH (Terminal/CLI)** | Standard method to connect to Linux instances via SSH. | - SSH client (Linux/Mac built-in, PuTTY for Windows)  - Key pair (.pem file)  - Public IP address or DNS | 1. Open terminal (or PuTTY).  2. Run: ssh -i <path\_to\_pem\_file> <username>@<public\_ip\_or\_dns> |

|  |  |  |  |
| --- | --- | --- | --- |
| **EC2 Instance Connect** | Connect directly from AWS Console using a browser. | - AWS Management Console  - Supported OS (Amazon Linux 2, Ubuntu)  - IAM permissions for Instance Connect | 1. Open AWS Console and go to EC2.  2. Select your instance and click "Connect."  3. Choose "EC2 Instance Connect" and click "Connect." |

|  |  |  |  |
| --- | --- | --- | --- |
| **Session Manager** | Connect via AWS Systems Manager without SSH. | - Instance must have SSM agent installed  - IAM role with SSM permissions  - No inbound rules needed | 1. Open AWS Console and go to EC2.  2. Select instance and click "Connect."  3. Choose "Session Manager" and click "Connect." |

|  |  |  |  |
| --- | --- | --- | --- |
| **RDP (for Windows)** | Connect to Windows instances using Remote Desktop Protocol. | - Remote Desktop Client (Windows built-in or rdp client)  - Username and password  - Public IP address or DNS | 1. Get the instance's public IP and Administrator password.  2. Open Remote Desktop and enter the IP.  3. Enter the username and password to connect. |

|  |  |  |  |
| --- | --- | --- | --- |
| **SSH via Bastion Host** | Connect to private instances through a public bastion host. | - SSH client  - Bastion host with public IP  - Key pair for both instances | 1. SSH into the bastion host: ssh -i <path\_to\_pem\_file> ec2-user@<bastion\_public\_ip>  2. From the bastion, connect to the private instance: ssh ec2-user@<private\_instance\_ip> |

|  |  |  |  |
| --- | --- | --- | --- |
| **Web-Based Console (AWS Console)** | Access the console directly through the AWS Management Console. | - AWS Management Console access  - IAM permissions | 1. Open the AWS Console.  2. Navigate to EC2 and select the instance.  3. Click on the "Connect" button. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Third-Party Tools** | Use tools like MobaXterm, Bitvise, or Cyberduck for SSH/SFTP. | - Third-party tool installed  - Key pair (.pem file) or username/password | 1. Open the third-party tool.  2. Configure a new session with the instance's public IP, username, and key file (or password). |

| **Method** | **Description** | **Pros** | **Cons** |
| --- | --- | --- | --- |

|  |  |  |  |
| --- | --- | --- | --- |
| **🔑 SSH (Command Line)** | Use SSH with a key pair to connect via terminal. | Secure, widely used, and customizable. | Requires terminal access and key management. |

|  |  |  |  |
| --- | --- | --- | --- |
| **🌐 EC2 Instance Connect** | Connect directly from the AWS Management Console. | No need for key pairs; browser-based. | Limited to supported OS (Amazon Linux 2, Ubuntu). |

|  |  |  |  |
| --- | --- | --- | --- |
| **💻 Session Manager** | Use AWS Systems Manager Session Manager for SSH. | No need for open ports; works with private instances. | Requires additional IAM permissions and setup. |

|  |  |  |  |
| --- | --- | --- | --- |
| **🌟 Remote Desktop (RDP)** | Connect to Windows instances using RDP. | GUI-based access for Windows users. | Requires RDP client; needs security group adjustments. |

|  |  |  |  |
| --- | --- | --- | --- |
| **🔌 AWS CLI** | Use the AWS Command Line Interface for connecting and managing instances. | Scriptable and can be automated. | Requires CLI setup and knowledge of AWS commands. |

|  |  |  |  |
| --- | --- | --- | --- |
| **📱 Third-party Tools** | Use tools like PuTTY (Windows) or MobaXterm for SSH access. | User-friendly interfaces. | Requires installation and configuration. |