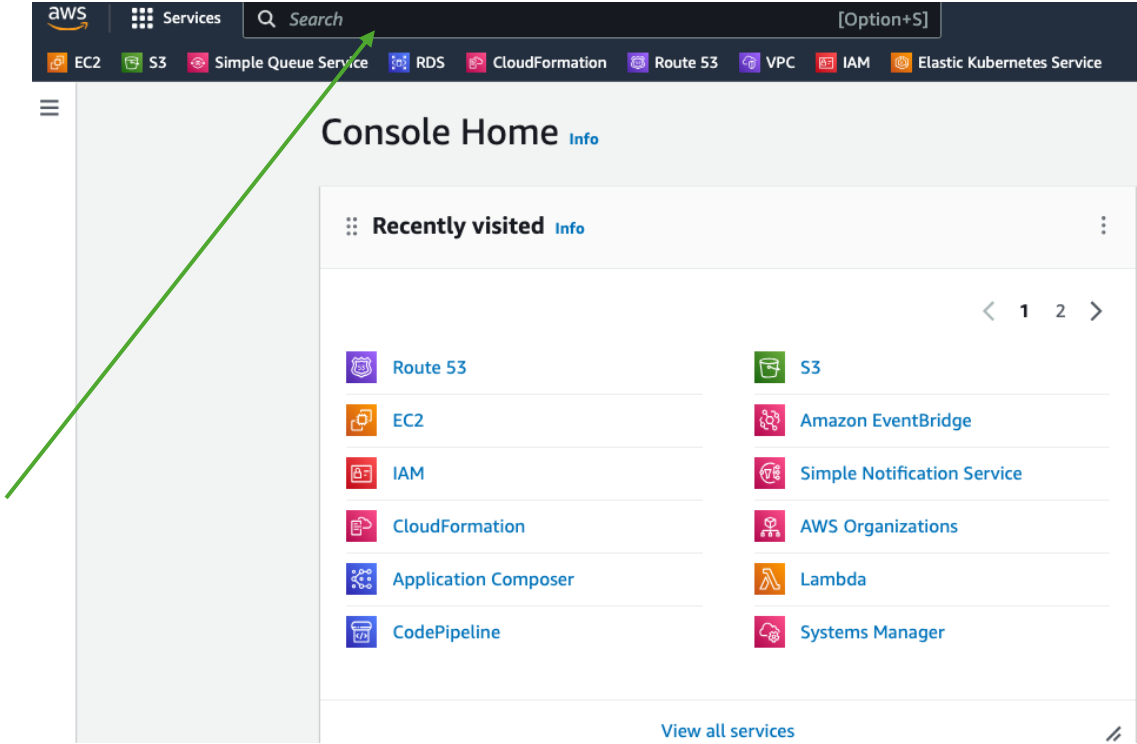
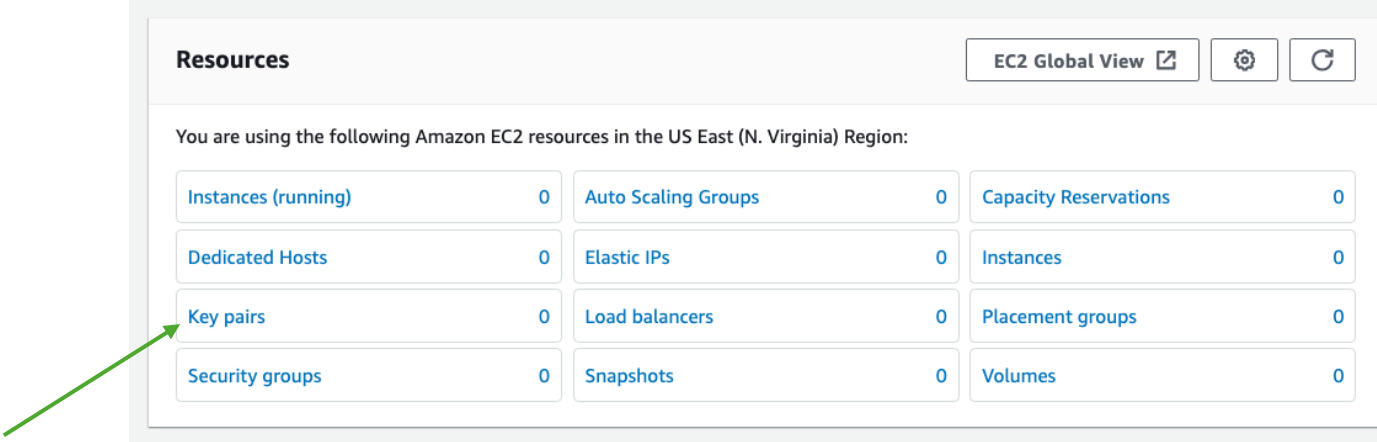


AWS EC2 Instance Run Book

- 1. Login to your AWS account following this link <https://console.aws.amazon.com/>
- 2. Search EC2 on the Search bar and select the EC2 service.



- 3. This will take you to the EC2 dashboard. From here click on Key pairs



- 4. Click the orange button 'Create key pair' to create a key pair.
 - a. Name: jjtech-linux (Please don't change the name)
 - b. Keep everything as default (Don't change anything)
 - c. Click 'Create key pair'. (This will automatically download a file called jjtech-linux.pem)

EC2 > Key pairs > Create key pair

Create key pair Info

Key pair

A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.

Name

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type Info

☒ RSA

☐ ED25519

Private key file format

☒ .pem

For use with OpenSSH

☐ .ppk

For use with PuTTY

Tags - optional

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel

Create key pair

5. Repeat step 2 to return to the EC2 dashboard
6. Click 'Launch instance' (If you don't see it scroll down your page)

Resources

EC2 Global View

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)

0

Auto Scaling Groups

0

Capacity Reservations

0

Dedicated Hosts

0

Elastic IPs

0

Instances

0

Key pairs

1

Load balancers

0

Placement groups

0

Security groups

0

Snapshots

0

Volumes

0

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance

Migrate a server

Note: Your instances will launch in the US East (N. Virginia) Region

Service health

AWS Health Dashboard

Region

US East (N. Virginia)

Status

This service is operating normally.

Zones

- a. Name: JJtech-linux-instance
- b. Key pair(login): select jjtech-linux

Name and tagsInfo

Name

jjtech-linux-instance

Add additional tags

▼ Application and OS Images (Amazon Machine Image)Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Q Search our full catalog including 1000s of application and OS images

Quick Start

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

SUSE L

SUS

Q

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI

Free tier eligible

ami-0ae8f15ae66fe8cda (64-bit (x86), uefi-preferred) / ami-0e36db3a3a535e401 (64-bit (Arm), uefi)

Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Architecture

64-bit (x86)

Boot mode

uefi-preferred

AMI ID

ami-0ae8f15ae66fe8cda

Verified provider

▼ Instance typeInfo | Get advice

Instance type

t2.micro

Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true

On-Demand Windows base pricing: 0.0162 USD per Hour

On-Demand SUSE base pricing: 0.0116 USD per Hour

On-Demand RHEL base pricing: 0.026 USD per Hour

On-Demand Linux base pricing: 0.0116 USD per Hour

All generations

Compare instance types

Additional costs apply for AMIs with pre-installed software

▼ 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

jjtech-linux

Create new key pair

Make sure a network is selected (The default network will be automatically selected)

▼ Network settings Info

Edit

Network Info

vpc-01480de77b23617d6

Subnet Info

No preference (Default subnet in any availability zone)

Auto-assign public IP Info

Enable

Additional charges apply when outside of free tier allowance

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-1' with the following rules:

☒ Allow SSH traffic from

Helps you connect to your instance

Anywhere
0.0.0.0/0

☐ 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.

×

- c. Click 'Launch instance'
- d. Click on the instance Id and it will take you to the instance

EC2 > Instances > Launch an instance

Success

Successfully initiated launch of instance (i-0efc98c714de8b7bf)

▶ Launch log

- e. Wait for the instance to initialized you will see a 2/2 checks passed

Instances (1) Info

Find Instance by attribute or tag (case-sensitive)

All states ▼

Instance ID = i-0efc98c714de8b7bf

×

Clear filters

<input type="checkbox"/>	Name ↗	Instance ID	Instance state	Instance type	Status check
<input type="checkbox"/>	jjtech-linux-in...	i-0efc98c714de8b7bf	Running	t2.micro	Initializing

- f. Select the instance and click connect

Instances (1/1) Info

Find Instance by attribute or tag (case-sensitive)

All states ▼

Instance ID = i-0efc98c714de8b7bf

×

Clear filters

<input checked="" type="checkbox"/>	Name ↗	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input checked="" type="checkbox"/>	jjtech-linux-in...	i-0efc98c714de8b7bf	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a

Refresh

Connect

g.

Connect to instance Info

Connect to your instance i-0efc98c714de8b7bf (jjtech-linux-instance) using any of these options

EC2 Instance Connect

Session Manager

SSH client

EC2 serial console

Instance ID

i-0efc98c714de8b7bf

 (jjtech-linux-instance)

1. Open an SSH client.

2. Locate your private key file. The key used to launch this instance is jjtech-linux.pem

3. Run this command, if necessary, to ensure your key is not publicly viewable.

chmod 400 "jjtech-linux.pem"

4. Connect to your instance using its Public DNS:

ec2-44-204-145-224.compute-1.amazonaws.com

Example:

ssh -i "jjtech-linux.pem" ec2-user@ec2-44-204-145-224.compute-1.amazonaws.com

Note:

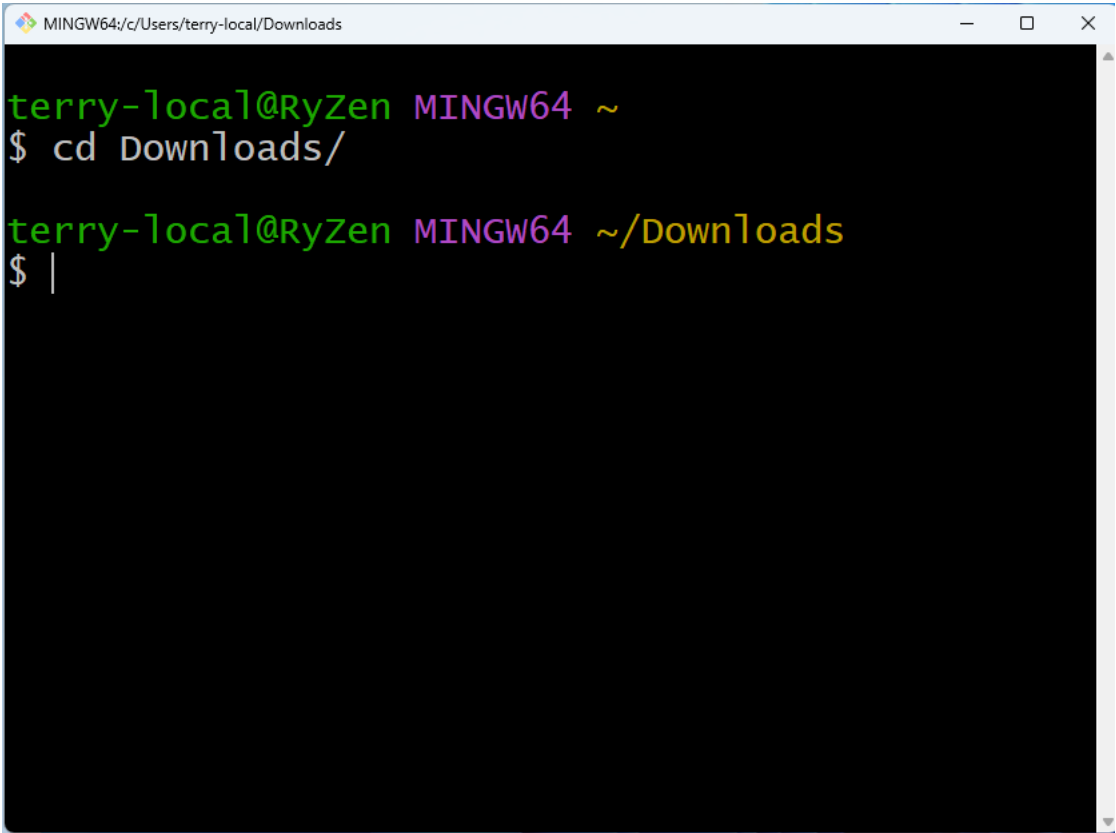
 In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

Cancel

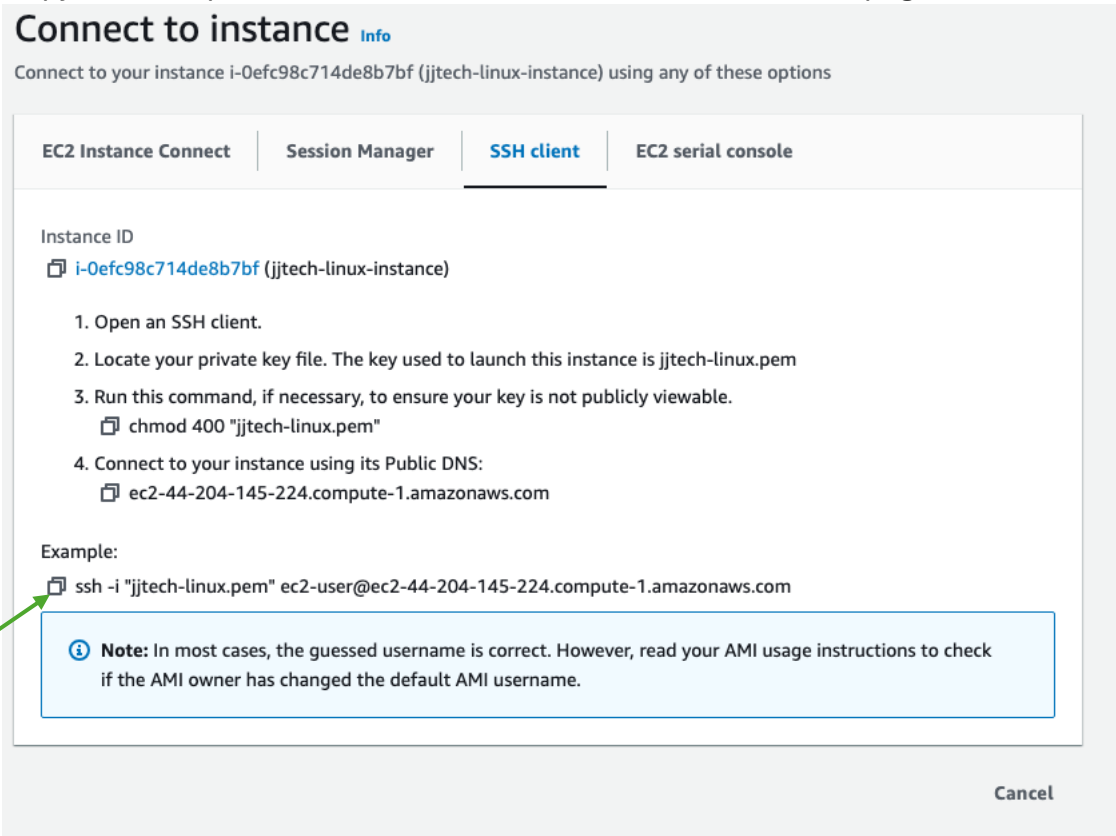
Mac Users skip to page 8

For Windows Users:

- 1. Open Git bash
- 2. cd to Downloads



- 3. Copy the example command found on the connect to instance page



- 4. Paste that command in Git bash and hit enter.
Type yes to accept the fingerprint

For Mac Users:

- 1. Open you terminal
cd to Downloads



- 2. On the Connect to instance page, copy the command to change the permission of the key and paste on your terminal

Connect to instance [Info](#)

Connect to your instance i-0efc98c714de8b7bf (jjtech-linux-instance) using any of these options

EC2 Instance Connect

Session Manager

SSH client

EC2 serial console

Instance ID

i-0efc98c714de8b7bf (jjtech-linux-instance)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is jjtech-linux.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
 `chmod 400 "jjtech-linux.pem"`
4. Connect to your instance using its Public DNS:
 ec2-44-204-145-224.compute-1.amazonaws.com

Example:

`ssh -i "jjtech-linux.pem" ec2-user@ec2-44-204-145-224.compute-1.amazonaws.com`

Note: In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

Cancel



