

Introduction

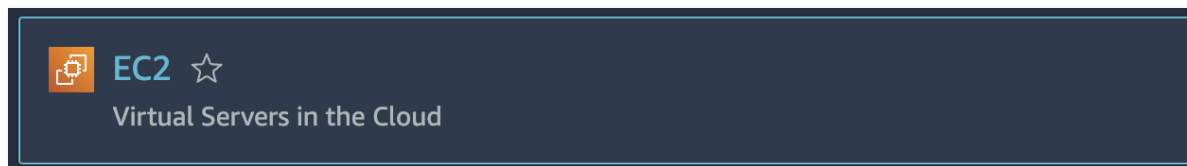
A bastion host is typically a host that sits inside your public subnet for the purposes of SSH (and/or RDP) access. You can think of it as a host for gaining secure access to resources in your VPC from the public internet. Bastion hosts are sometimes referred to as jump servers, as you jump to one, then back out of it.

Once you access a bastion host (for example, by using SSH to log into it), in order to access other instances you must either set up SSH port forwarding or copy your SSH key material to the bastion host. The latter is not ideal for security reasons in a production environment. If you require Windows connectivity, then setting up Remote Desktop Gateway instead of SSH port forwarding is recommended. This lab step assumes SSH connectivity to Linux instances.

In this lab step, you will create an EC2 instance that will serve as both an observer instance that you can run various tests from and a bastion host.

Instructions

1. In the AWS Management Console search bar, enter *EC2*, and click the **EC2** result under **Services**:



2. To see available instances, click **Instances** in the left-hand menu:



3. Click **Launch instances**:

An orange rectangular button with the text "Launch instances" in white, bold, sans-serif font.

4. In the **Name and tags** section, enter *bastion* under **Name**.


5. In the **Application and OS Images** section, select the **Amazon Linux** option under **Quick Start**:

▼ 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

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


Quick Start




Amazon
Linux




Ubuntu




Windows




Red Hat



SUSE Linux





[Browse more AMIs](#)

Including AMIs from
AWS, Marketplace and
the Community

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type

ami-0ca285d4c2cda3300 (64-bit (x86)) / ami-0f48d15c9efb5f63d (64-bit (Arm))

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

Free tier eligible ▼

Description

Amazon Linux 2 Kernel 5.10 AMI 2.0.20220426.0 x86_64 HVM gp2

Architecture

AMI ID

ami-0ca285d4c2cda3300

64-bit (x86) ▼

ami-0ca283d4c2cda3300

6. In the **Instance Type** section, you should not change any options. Simply make sure the default **t2.micro** is selected:

Instance type

t2.micro
Family: t2 1 vCPU 1 GiB Memory
On-Demand Linux pricing: 0.0116 USD per Hour
On-Demand Windows pricing: 0.0162 USD per Hour

Free tier eligible ▼

[Compare instance types](#)

7. In the **Key pair** section, select the `338139317922` keypair:

▼ 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

Select ▲

Q

Proceed without a key pair (Not recommended) Default value

226375879776
Type: rsa

↻ Create new key pair

Edit

Note: Your keypair may differ from the screenshot.

Reminder: The PEM or PPK formatted key pair can be downloaded directly from the **Your lab data** section of the Cloud Academy Lab page at any time.

8. In the **Network settings** section, click **Edit**, and configure the following instance details:

- **VPC:** Select the **cloudacademy-labs** VPC
- **Subnet:** Select the **Public-A | us-west-2a** subnet
- **Auto-assign Public IP:** Select **Enable**
- **Firewall:** Select **Create security group**
- **Security group name:** Enter *SG-bastion*
- **Description:** Enter *SG for bastion host. SSH access only*
- **Type:** SSH
- **Protocol:** TCP
- **Port:** 22
- **Source type:** Anywhere
- **Source:** 0.0.0.0/0

Note: It isn't a best practice to set the source to any IP, but is used to allow the lab to work in complex network environments. If you are in an environment with a static IP, you could set the source field to My IP in the drop-down menu to only allow your IP for improved security.

9. Review the **Summary** section and click **Launch instance**:

A rectangular button with an orange background and the text "Launch instance" in white, bold font.

A confirmation page will let you know that your instance is launching:

**Success**

Successfully initiated launch of instance ([i-087e62712e358d508](#))

► **Launch log**

10. Click **View all instances** at the bottom of the confirmation page. The status of your instance will transition to **Running** within 30 seconds.

Summary

In this lab step, you launched an EC2 instance with a public IP address in your public subnet that will be used as a bastion host.

In a production environment, you would restrict inbound access to specific IP addresses of your network administrators. The outbound traffic will also be modified later in this lab, restricting the destination to the security group of instances in your private subnet only. When configuring bastion hosts, they are often stripped down to provide the minimum amount of services.