

How To Launch an EC2 Instance on AWS.

Step 1: Log in to AWS Management Console

1. Go to the [AWS Management Console](#).
2. Log in with your credentials.

Step 2: Navigate to EC2 Service

1. In the AWS Management Console, search for **EC2** in the search bar and click on it.
2. This will take you to the EC2 Dashboard.

Step 3 : Launch an Instance

1. On the EC2 Dashboard, click **Launch Instance**.
2. You'll be directed to the "Launch an Instance" wizard.

Step 4 : Configure Instance Details

1. **Name and Tags :**
 - Give your instance a name by entering a value in the "Name" field.
 - Optionally, add tags to categorize your instance.
2. **Select AMI (Amazon Machine Image):**
 - Choose an operating system (e.g., Amazon Linux, Ubuntu, Windows Server).
 - Free-tier users can select the Amazon Linux 2 AMI (Free Tier Eligible).
3. **Choose Instance Type :**
 - Select an instance type based on your use case (e.g., t2.micro for free-tier eligibility).
 - Click **Next** to proceed.

Step 5 : Configure Key Pair

1. If you don't have a key pair:
 - Click **Create new key pair**.
 - Enter a name and select the format (PEM for Linux, PPK for Windows).
 - Download the key pair and keep it secure (it's used to connect to the instance).
2. If you already have a key pair:
 - Select it from the dropdown.

Step 6 : Configure Network Settings

1. VPC and Subnet :

- Choose a VPC (default is available) and a subnet.

2. Auto-assign Public IP :

- Ensure it's enabled if you want the instance to be accessible over the internet.

3. Security Groups :

- Create a new security group or use an existing one.
- Add rules for necessary access, e.g., SSH (port 22) for Linux or RDP (port 3389) for Windows.

Step 7 : Add Storage

1. Configure the instance's storage.

- Default storage is often sufficient for basic use.
- Add additional volumes if needed.

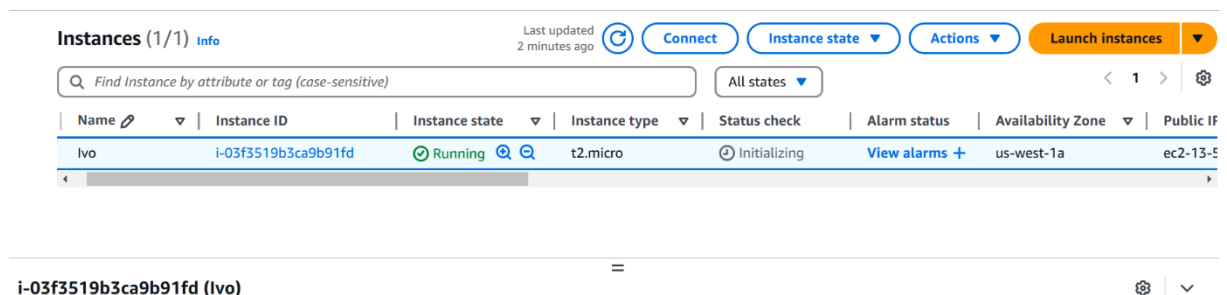
2. Ensure you stay within free-tier limits if applicable.

Step 8 : Review and Launch

1. Review all the details you configured.
2. Click **Launch Instance**.

Step 9 : Monitor Instance Launch

1. After clicking "Launch Instance," you'll be redirected to a page showing the instance ID and status.
2. Wait for the instance state to change to **Running**.



The screenshot displays the AWS Management Console 'Instances' page. At the top, there's a header with 'Instances (1/1)' and an 'Info' link. To the right, it shows 'Last updated 2 minutes ago' and several action buttons: 'Connect', 'Instance state' (with a dropdown), 'Actions' (with a dropdown), and 'Launch instances' (in orange). Below this is a search bar with the placeholder 'Find Instance by attribute or tag (case-sensitive)' and a filter dropdown set to 'All states'. The main content is a table with columns: Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IP. A single instance 'lvo' is listed with ID 'i-03f3519b3ca9b91fd', state 'Running' (indicated by a green checkmark), type 't2.micro', status check 'Initializing', alarm status 'View alarms +', availability zone 'us-west-1a', and public IP 'ec2-13-5...'. Below the table, the instance name 'i-03f3519b3ca9b91fd (lvo)' is shown again.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
lvo	i-03f3519b3ca9b91fd	Running	t2.micro	Initializing	View alarms +	us-west-1a	ec2-13-5...

How To Attach Security Group to My Instance.

Step 1: Identify your Public IP

1. Visit a site like [WhatIsMyIP](#) or search "What is my IP" in a browser.
2. Note down your public IP address (e.g., 203.0.113.25).

Step 2: Log in to AWS Management Console

1. Go to the [AWS Management Console](#).
2. Navigate to the **EC2 Dashboard** by searching for "EC2" in the search bar.

Step 3: Locate the Security Group

1. On the EC2 Dashboard, find the **Security Groups** option under the **Network & Security** section in the left-hand menu.
2. Click on **Security Groups**.

Step 4: Create or Edit a Security Group

1. **To Create a New Security Group:**
 - Click **Create Security Group**.
 - Provide a name and description for the security group.
 - Ensure it is associated with the correct VPC.
2. **To Edit an Existing Security Group:**
 - Select the security group you want to modify and click on **Edit Inbound Rules**.

Step 5 : Configure Inbound Rules

1. Add a new rule with the following details:
 - **Type** : SSH
 - **Protocol**: TCP (auto-filled for SSH)
 - **Port Range** : 22
 - **Source** : Select **My IP**.

AWS will automatically detect your current public IP and append /32 to allow access only from your machine (e.g., 203.0.113.25/32).

Security Groups (1/3) Info			
<div> <div>Find resources by attribute or tag</div> <div>< 1 > ⚙</div> </div>			
<div> <div> <div></div> <div>Name</div> </div> <div> <div></div> <div>Security group ID</div> </div> <div> <div></div> <div>Security group name</div> </div> <div> <div></div> <div>VPC ID</div> </div> </div>			
<div> <div></div> <div></div> </div>			
<div>Details</div>			
<div>Security group name</div> <div>ssh-ivo##</div>	<div>Security group ID</div> <div>sg-00fa2e861da5a7198</div>	<div>Description</div> <div>Allows SSH access to developers</div>	<div>VPC ID</div> <div>vpc-0c31038cfd91bfa60</div>
<div>Owner</div> <div>463470955614</div>	<div>Inbound rules count</div> <div>1 Permission entry</div>	<div>Outbound rules count</div> <div>0 Permission entries</div>	

Purpose of a Keypair.

A key pair in AWS is used to enable secure access to Amazon EC2 instances. It serves as the authentication mechanism for logging in to your instance, especially for Linux-based EC2 instances using **SSH** (Secure Shell).

Key Pair Components

A key pair consists of:


- Public Key :
- Stored by AWS and associated with the EC2 instance during creation.
 - Embedded into the instance's **authorized keys** file (for Linux/UNIX instances) during launch.
 - Cannot be downloaded; AWS manages it internally.
- Private Key :
- Generated by AWS or your own system (if you create and import a key pair).
 - Must be securely stored by the user, as AWS does not retain it.
 - Used by the client (e.g., your local machine) to establish an SSH connection to the instance.

Key pairs (1/1) Info					
Find Key Pair by attribute or tag					
<div> <div> <div></div> <div>Actions</div> </div> <div>Create key pair</div> </div>					
<div> <div><</div> <div>1</div> <div>></div> <div></div> </div>					
<input checked="" type="checkbox"/>	Name	Type	Created	Fingerprint	ID
<input checked="" type="checkbox"/>	bakor	rsa	2024/11/29 13:27 GMT+1	97:02:38:ff:9d:dc:5d:a4:...	key-051a2a89efd70d9d5

How To Create and Modify the IAM Role.

Step 1 : Create an IAM Role

- Navigate to the IAM Console:**
 - Go to the [IAM Dashboard](#).
- Create a New Role :**
 - Click on **Roles** in the left-hand menu, then click **Create Role**.
- Select Trusted Entity :**
 - Choose **AWS Service** and select **EC2** as the trusted entity type.
- Attach Policies to the Role:**
 - Select the managed policies that provide the necessary permissions (e.g., AmazonS3ReadOnlyAccess or custom permissions). You can skip this step if you plan to attach inline policies later.
- Name the Role :**
 - Give the role a descriptive name (e.g., EC2S3AccessRole) and complete the creation process.

Permissions					Trust relationships	Tags	Last Accessed	Revoke sessions
Permissions policies (1) Info					<div> <div> <div></div> <div>Simulate</div> </div> <div>Remove</div> <div>Add permissions</div> </div>			
You can attach up to 10 managed policies.								
<div> <div>Search</div> <div>Filter by Type</div> <div>All types</div> </div>					<div> <div><</div> <div>1</div> <div>></div> <div></div> </div>			
<input type="checkbox"/>	Policy name	Type	Attached entities					
<input type="checkbox"/>	 AmazonS3FullAccess	AWS managed	1					

How to create an Inline policy and attach to a role.

Step 1: Create the Role (if not already created)

1. **Log in to AWS Console.**
2. Go to the [IAM Dashboard](#).
3. Select **Roles** from the left-hand menu.
4. Click **Create Role** and choose a **trusted entity** (e.g., EC2, Lambda).
5. Add any required **AWS Managed Policies** during this step (optional).
6. Name the role and complete the process.

Step 2: Create and Attach an Inline Policy

1. **Locate the Role :**
 - In the IAM Dashboard, click **Roles**.
 - Find and select the role to which you want to attach the inline policy.
2. **Attach Inline Policy :**
 - Scroll down to the **Permissions** tab and click **Add permissions > Create inline policy**.
3. **Define the Policy :**
 - Use either the **Visual Editor** or the **JSON Editor** to define the policy.
 - Example JSON for S3 Read-Write access to a specific bucket:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource": "arn:aws:s3:::example-bucket/*"
    }
  ]
}
```

4. **Review and Attach :**
 - Click **Review Policy**, name the policy (e.g., S3InlinePolicy), and save it.

Permissions policies (1)
[Info](#)

Simulate
Remove
Add permissions

You can attach up to 10 managed policies.

Filter by Type
All types

☐

Policy name

☐

Type

☐

Attached entities

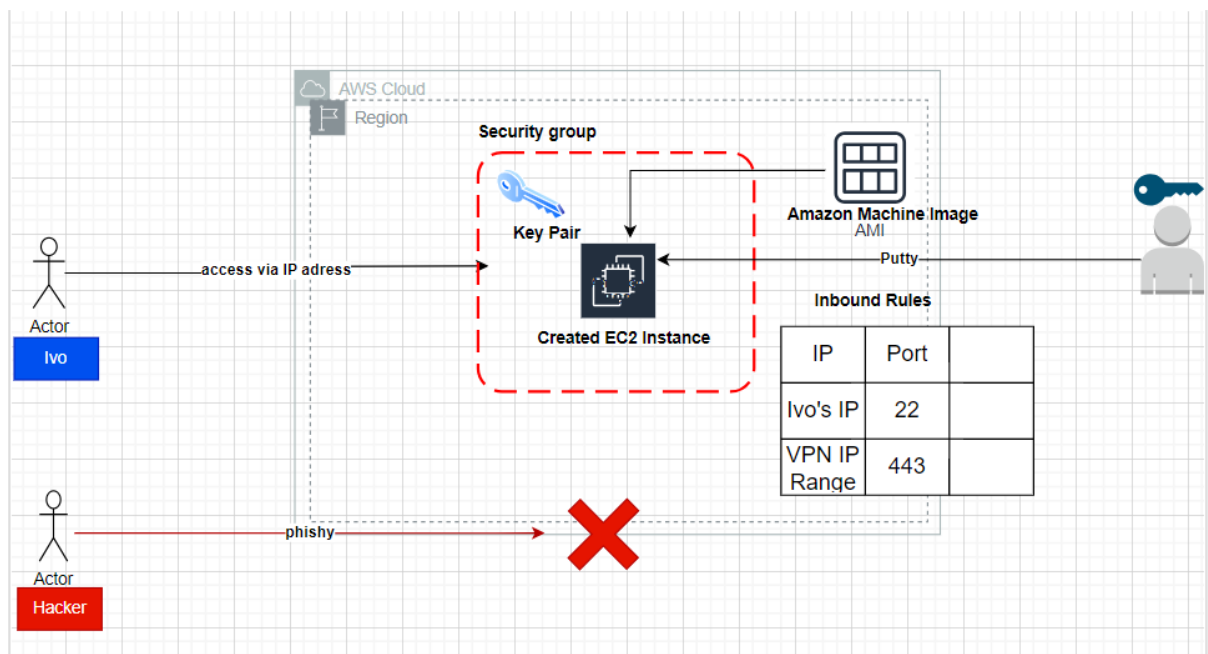
☐
☒
[customes3access](#)
Customer inline
0

▶ **Permissions boundary** (not set)

▼ **Generate policy based on CloudTrail events**

You can generate a new policy based on the access activity for this role, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. [Learn more](#)

AWS Illustration.



Final Work.

Instances (1/1) Info

Last updated 2 minutes ago

Connect

Instance state

Actions

Launch instances

Find Instance by attribute or tag (case-sensitive)

All states

< 1 >

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Pul
<input checked="" type="checkbox"/>	Ivo	i-03f3519b3ca9b91fd	Running	t2.micro	2/2 checks passed	View alarms	us-west-1a	ec2

i-03f3519b3ca9b91fd (Ivo)

IAM Role

mycustomrole

Owner ID

463470955614

Launch time

Fri Nov 29 2024 13:28:45 GMT+0100 (Central European Standard Time)

Security groups

sg-05cc471959125e74a (launch-wizard-1)