**How To Launch an EC2 Instance on AWS.**

**Step 1: Log in to AWS Management Console**

1. Go to the [AWS Management Console](https://aws.amazon.com/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**

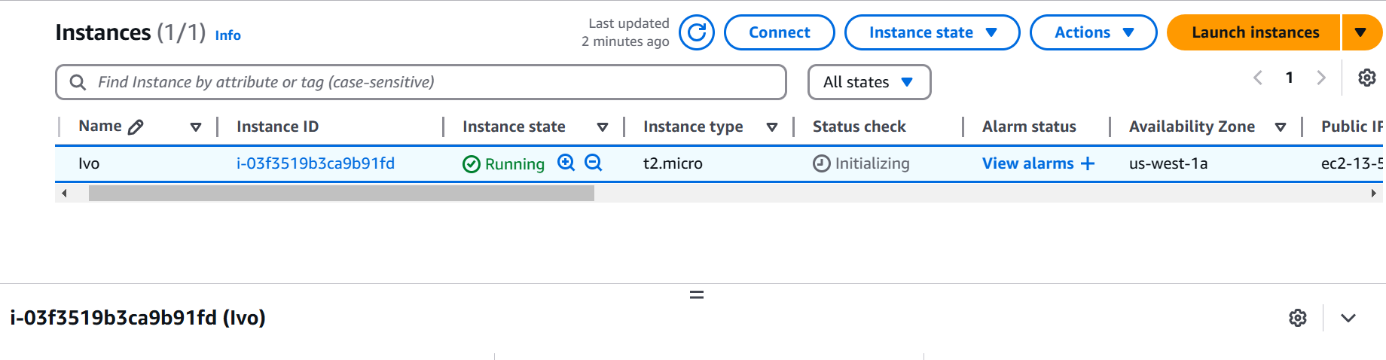
1. Configure the instance’s storage.
   * Default storage is often sufficient for basic use.
   * Add additional volumes if needed.
2. Ensure you stay within free-tier limits if applicable.

**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**.



**How To Attach Security Group to My Instance.**

### **Step 1: Identify your Public IP**

1. Visit a site like [WhatIsMyIP](https://whatismyipaddress.com/) 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](https://aws.amazon.com/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**.

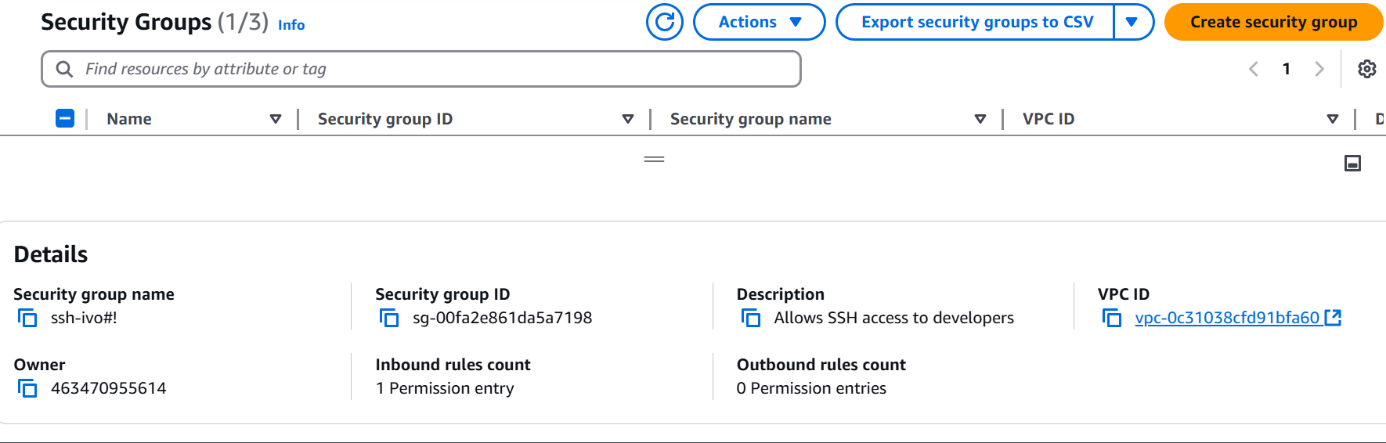
**Step 4: Create or Edit a Security Group**

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).



**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**

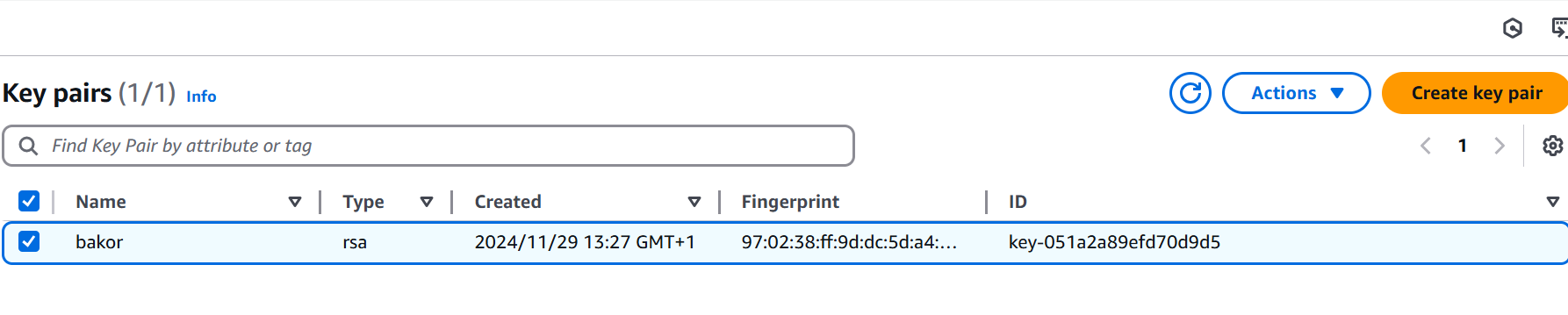
A key pair consists of:

 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** :

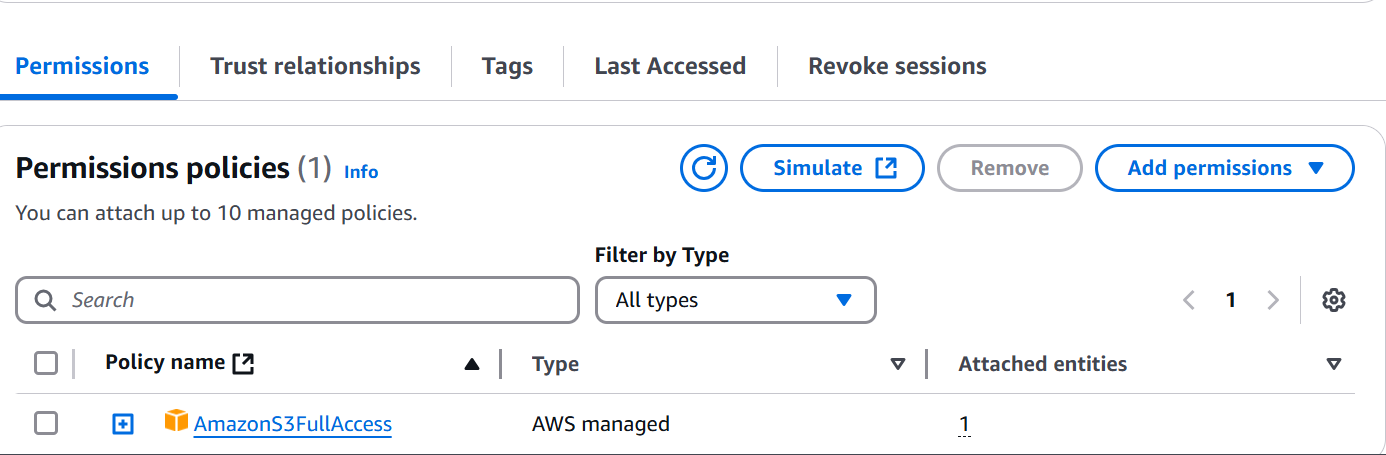
* Generated by AWS or your own system (if you create and import a key pair).
* Must be securely stored by the user, as AWS does not retain it.
* Used by the client (e.g., your local machine) to establish an SSH connection to the instance.



**How To Create and Modify the IAM Role.**

**Step 1 : Create an IAM Role**

1. **Navigate to the IAM Console**:
   * Go to the [IAM Dashboard](https://console.aws.amazon.com/iam/).
2. **Create a New Role** :
   * Click on **Roles** in the left-hand menu, then click **Create Role**.
3. **Select Trusted Entity** :
   * Choose **AWS Service** and select **EC2** as the trusted entity type.
4. **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.
5. **Name the Role** :
   * Give the role a descriptive name (e.g., EC2S3AccessRole) and complete the creation process.



**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](https://console.aws.amazon.com/iam/).
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"

],

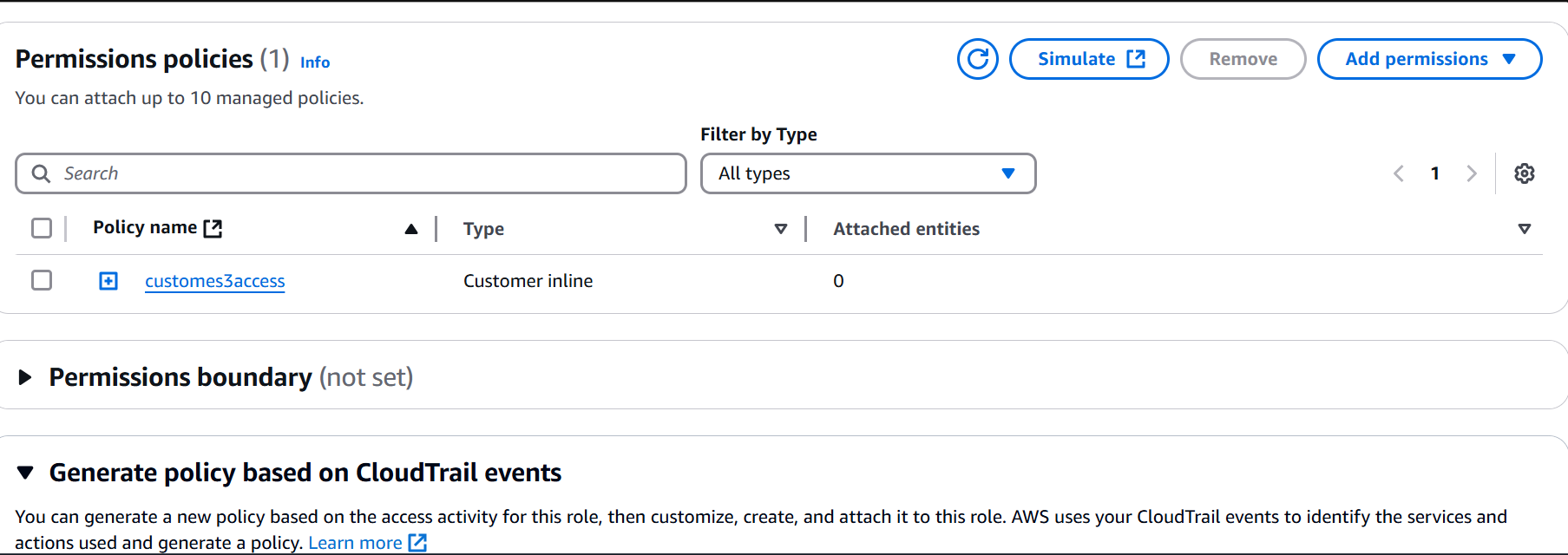
"Resource": "arn:aws:s3:::example-bucket/\*"

}

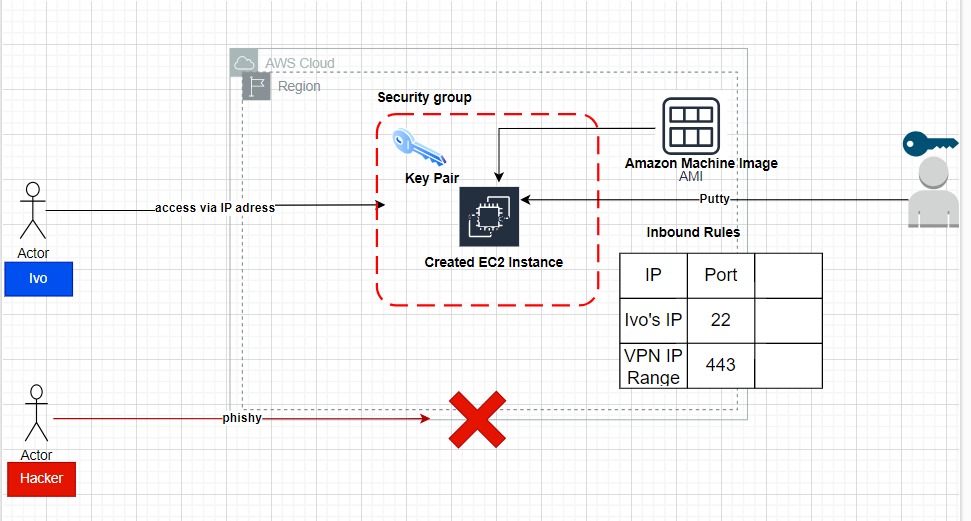
]

}

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



**AWS Illustration.**

****

**Final Work.**

