How to create an EC2 instance on the AWS Console

Here are the steps to create an EC2 instance on the AWS Console:

1. **Login to AWS Console**:
   - Navigate to AWS Management Console.
   - Sign in with your credentials.
2. **Open EC2 Service**:
   - In the console, search for **EC2** in the services search bar and click on it.
3. **Launch an Instance**:
   - Click on the **Launch Instance** button.
4. **Configure Instance**:
   - **Name**: Provide a name for your instance.
   - **AMI (Amazon Machine Image)**: Choose an operating system (e.g., Amazon Linux, Ubuntu, etc.).
   - **Instance Type**: Select the desired instance type (e.g., t2.micro for free tier).
   - **Key Pair**: Create or select an existing key pair for SSH access.
   - **Network Settings**: Configure security group rules (allow SSH, HTTP/HTTPS if needed).
5. **Storage**:
   - Specify the root volume size and type (default is 8GB for many AMIs).
6. **Review and Launch**:
   - Double-check all configurations.
   - Click **Launch Instance**.
7. **Access the Instance**:
   - Use the public IP address and the key pair to connect via SSH or other methods.

To attach a security group with an inbound rule allowing **port 22 (SSH)** from your **IP address**, follow these steps:

After Instance Launch (Attach Security Group to an Instance)

1. **Access EC2 Dashboard**:
   - Navigate to the **Instances** section.
2. **Select Instance**:
   - Click on the instance ID to open its details.
3. **Modify Security Groups**:
   - Under the **Security** tab, click **Edit security groups**.
   - Attach the security group with the **SSH rule (port 22)** for your IP address.
   - Click **Save**.

Now, your instance will accept SSH connections only from your IP on port 22.

Key Pairs in AWS

A **key pair** in AWS is used for secure authentication when connecting to an EC2 instance via SSH. It consists of two components:

1. **Public Key**:
   - Stored on the EC2 instance during its creation.
   - Used to verify the identity of the user attempting to connect.
2. **Private Key**:
   - Downloaded and stored securely by you.
   - Used to authenticate your access to the EC2 instance.

Purpose of the Key Pair:

- **Secure SSH Connection**: Ensures that only users with the correct private key can access the instance.
- **Passwordless Login**: Instead of using a password, the private key is used to authenticate the connection, enhancing security.
- **Encryption**: The private and public key pair enables encrypted communication between your device and the EC2 instance.

Important Notes:

- The private key is **not retrievable** after creation. If lost, you cannot connect to the instance unless a new key pair or alternative authentication method is configured.
- Keep the private key safe and secure, as anyone with access to it can connect to your instance.

Create AWS IAM Roles

To create an AWS IAM role via the AWS Management Console, do the following:

---

1. Open the IAM Console

- Navigate to the AWS IAM Console.
- Sign in with an account that has permissions to create roles.

---

2. Select "Roles"

- In the left-hand navigation menu, click **Roles**.

---

3. Click "Create Role"

- On the Roles page, click the **Create role** button.

---

4. Choose Trusted Entity

- **AWS Service**: For roles used by AWS services (e.g., EC2, Lambda).

After selecting, click **Next**.

---

5. Attach Permissions Policies

- Choose one or more policies to define what the role can access.
  - Example: Select **AmazonS3ReadOnlyAccess** to grant read-only access to S3.
- Click **Next**.

---

7. Name and Review the Role

- Provide a **Role Name** (e.g., `MyEC2S3AccessRole`).
- Review the summary to ensure the configuration is correct.

---

8. Create the Role

- Click **Create role** to complete the process.

---

9. Use the Role

- Attach the role to an AWS resource (e.g., an EC2 instance or Lambda function).
- Ensure the resource has permissions to assume the role.

Attach an inline policy to an AWS Role

To attach an inline policy to an AWS IAM role using the AWS Management Console, follow these steps:

---

1. Open the IAM Console

- Go to the AWS IAM Console.

---

2. Locate the Role

- In the IAM dashboard, click **Roles** from the left-hand navigation.
- Search for and click on the role to which you want to attach an inline policy.

---

3. Access the Permissions Tab

- On the role's detail page, go to the **Permissions** tab.

---

4. Add an Inline Policy

- Click on the **Add Permissions** dropdown
- Select **Create inline policy**.

---

5. Define the Policy

- Use one of the following methods to define the policy:
  - **Visual Editor**:
    - Select the service (e.g., S3, EC2).
    - Specify actions (e.g., `ListBucket`, `GetObject` for S3).
    - Define resources (e.g., a specific S3 bucket ARN or * for all resources).
  - **JSON Editor**:
    - Switch to the JSON tab and paste your policy document. Example:

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

```
            }
        ]
    }
```

---

6. Review and Save

- Click **Next** to validate the policy.
- Provide a name for the inline policy (e.g., `S3AccessPolicy`).
- Click **Create Policy** to attach it to the role.

---

7. Verify the Policy

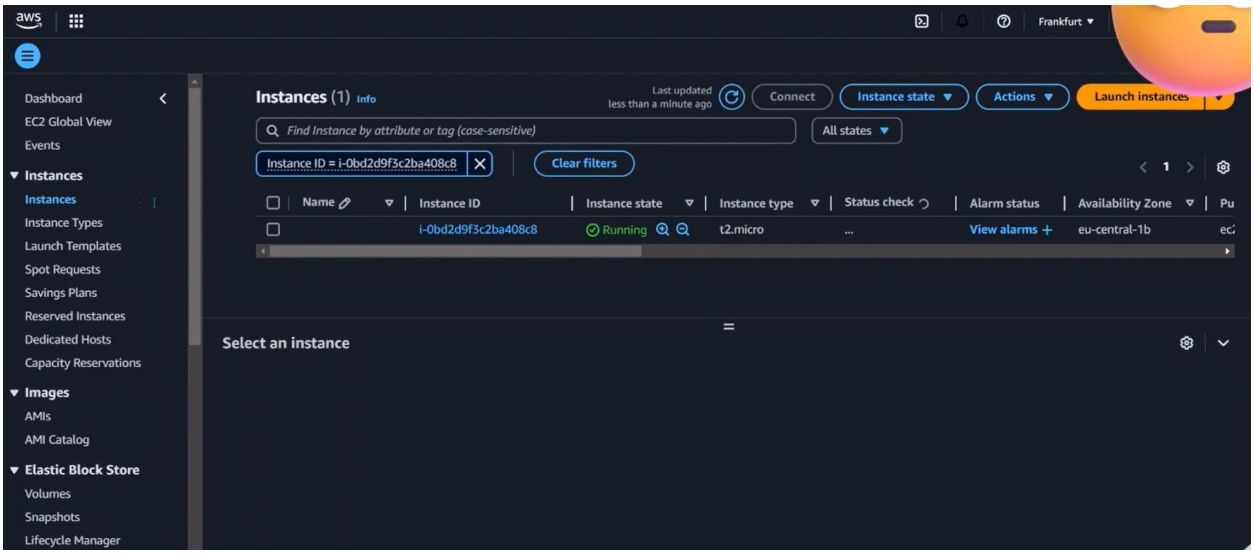
- Return to the role's **Permissions** tab and confirm that the inline policy is listed under the **Inline Policies** section.

Note:

- **Inline policies** are specific to the role they are attached to and cannot be shared or reused.
- For reusable policies, consider attaching **managed policies** instead.

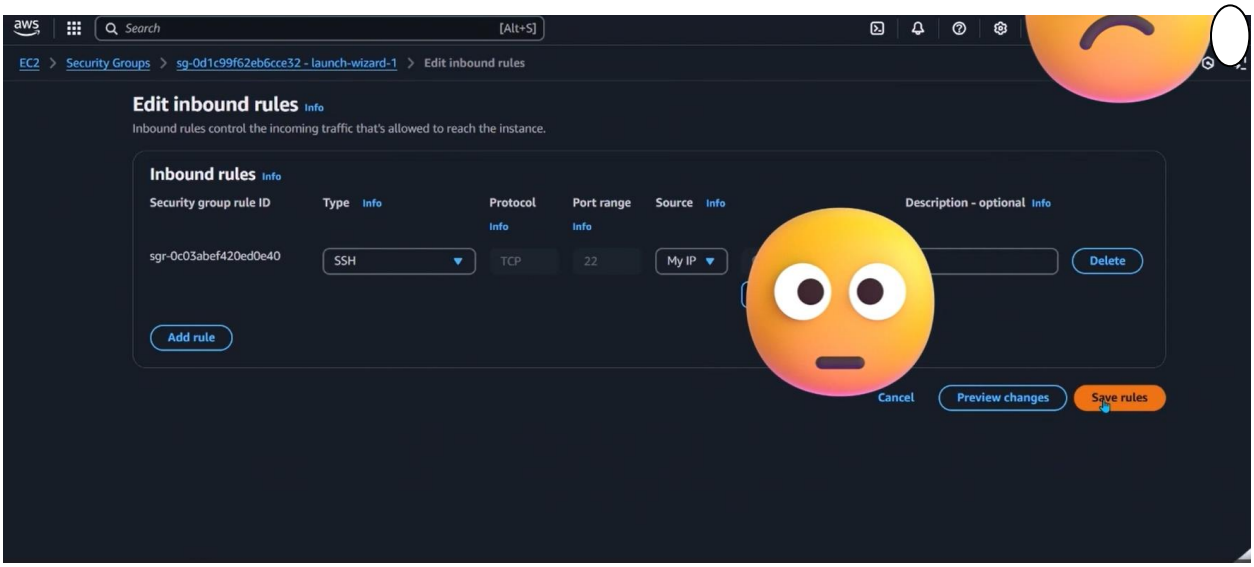
Practice

1. Creating an EC2 Instance



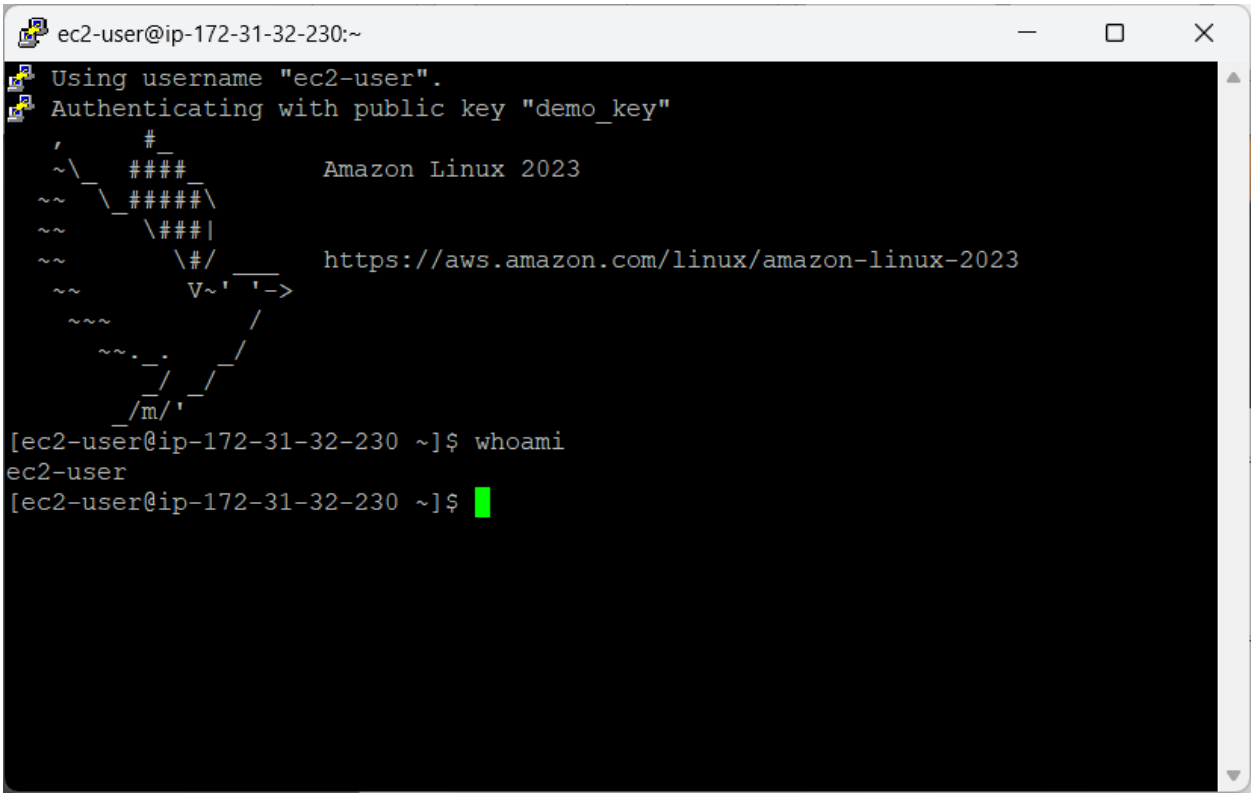
---

2. Modify Security Groups



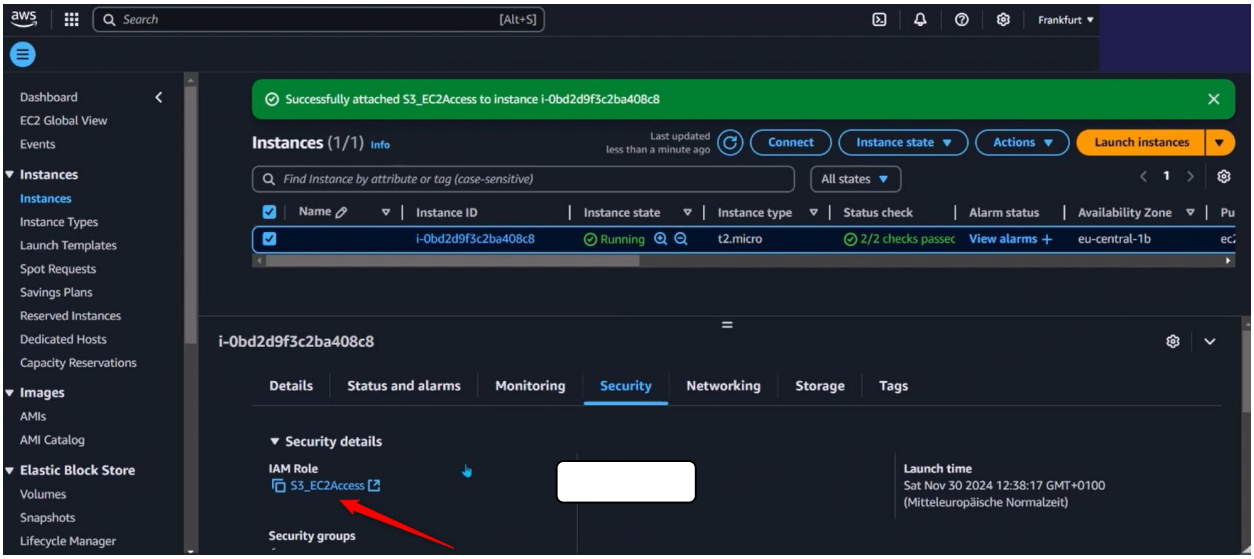
---

3. Connect to instance via puTTy



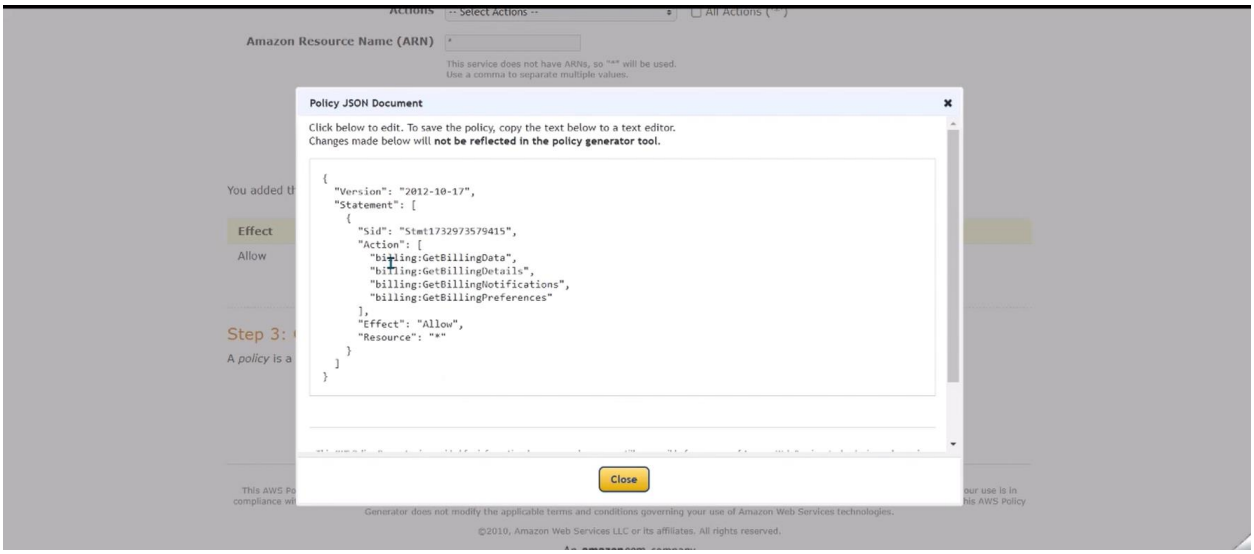
---

4. Create and Attach role to Instance



---

4. Attach inline policy to Role



---

5. Illustrated Summary with draw.io