

Deployment of Image

This project uses [AWS EC2](#). Below are the steps taken to use the meme-inspector image.

1. Choose AMI

2. Choose Instance Type

3. Configure Instance

4. Add Storage

5. Add Tags

6. Configure Security Group

7. Review

Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Q Search for an AMI by entering a search term e.g. "Windows"

Search by Systems Manager parameter

Quick Start

My AMIs

AWS Marketplace

Community AMIs

Meme-Inspector (AWS Linux NodeJS Express Nginx Svelte) - ami-0e281a18d980a13b9

Root device type: ebs

Virtualization type: hvm

Owner: 734841041858

ENA Enabled: Yes

Select

64-bit (x86)

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by:

All instance families

Current generation

Show/Hide Columns

Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)

	Family	Type	vCPUs
	t2	t2.nano	1
	t2	t2.micro Free tier eligible	1

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group:

Create a new security group

Select an existing security group

Security Group ID	Name	Description	Actions
<input type="checkbox"/> sg-0ffb2671	default	default VPC security group	Copy to new
<input checked="" type="checkbox"/> sg-04b029c3399cdc081	SSH and HTTP	SSH and HTTP	Copy to new

Warning

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.

Inbound rules for sg-04b029c3399cdc081 (Selected security groups: sg-04b029c3399cdc081)

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	
HTTP	TCP	80	:::0	
SSH	TCP	22	0.0.0.0/0	

Cancel

Previous

Review and Launch

Select an existing key pair or create a new key pair



A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance. Amazon EC2 supports ED25519 and RSA key pair types.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair



Select a key pair

cad_meme_inspector | RSA



☒ I acknowledge that I have access to the corresponding private key file, and that without this file, I won't be able to log into my instance.

[Cancel](#)

[Launch Instances](#)