

RUNNING DOCKER ON AWS EC2 INSTANCE AND DEPLOY A STATIC HTML PAGE THROUGH ECS

Launch an EC2 instance through AWS console with desired OS (preferably Ubuntu)
Create a new key pair on the launch window. A file with key pair will be downloaded on your local machine that's used to get the SSH session of the instance.

The screenshot displays the AWS Management Console interface. At the top, a 'Key pair (login)' section provides instructions and a 'Create new key pair' button. Below this, a 'Create key pair' modal is open, allowing the user to specify a key pair name, type (RSA or ED25519), and private key file format (.pem or .ppk). A warning box advises storing the private key securely. At the bottom, the 'Instances' table shows a single instance named 'docker-server' in a 'Running' state, with a 'Connect' button available.

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 ↕ ↻ Create new key pair

Create key pair ✕

Key pair name

Key pairs allow you to connect to your instance securely.

Enter key pair name

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

☒ **RSA**
RSA encrypted private and public key pair

☐ **ED25519**
ED25519 encrypted private and public key pair

Private key file format

☒ **.pem**
For use with OpenSSH

☐ **.ppk**
For use with PuTTY

⚠ When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. [Learn more](#)

Cancel Create key pair

Instances (1/1) Info Last updated less than a minute 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
<input checked="" type="checkbox"/>	docker-server	i-021fef6b64ea52fb4	Running	t2.micro	Initializing	View alarms +

Once the instance is launched, connect to the EC2 instance by selecting the server and clicking on connect button. Then go to the SSH client tab and copy the example command.

Now open terminal and change directory to where the key pair file is located.
Run the command so you can enter the SSH session of the EC2 instance.

In the SSH session of EC2 instance, download Docker engine for Ubuntu. Instructions to install Docker engine can be found on official Docker page.

<https://docs.docker.com/engine/install/ubuntu/>

Now that your EC2 instance has Docker installed, we are ready to dockerize the application. Change directory to where your source code is.

I have a very basic HTML page

```
<!DOCTYPE html>
<html>
<head>
<title>My HTML Page</title>
</head>
<body>

<h1>Welcome to My Website</h1>
<p>This is a test HTML page which I will be using in my projects.</p>

</body>
</html>
```

Now create a Dockerfile to build image with your source code.

```
FROM nginx:latest

COPY . /usr/share/nginx/html

EXPOSE 80

CMD ["nginx", "-g", "daemon off;"]
```

Now in order to push the image to AWS Elastic Container Registry, first install AWS CLI in your EC2 instance

```
curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
unzip awscliv2.zip
sudo ./aws/install
```

In AWS Console, create an IAM user with policy

“AmazonEC2ContainerRegistryFullAccess” assigned to it. This policy will give full access to the ECR to user.

Set permissions
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

- ☐ Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
- ☐ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.
- ☒ Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1/1317) [Create policy](#)

Choose one or more policies to attach to your new user.

Filter by Type: All types 1 match

Policy name	Type	Attached entities
<input checked="" type="checkbox"/> AmazonEC2ContainerRegi...	AWS managed	1

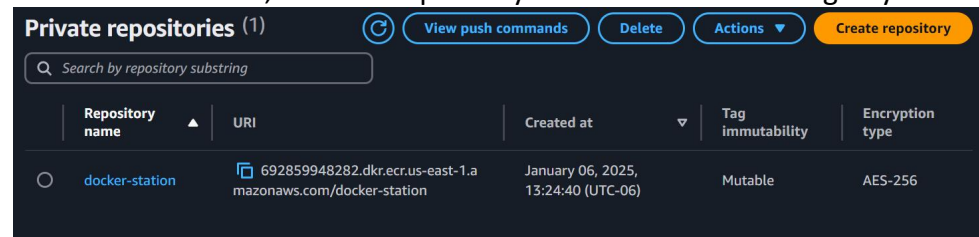
▶ Set permissions boundary - optional

Cancel Previous Next

Once the user is created, generate access key for the user and save the access key and secret access key.

In the terminal, create the credentials by running 'aws configure' command and use the access key and secret access key that we generated in the preceding step.

In the AWS console, create a repository in Elastic Container Registry

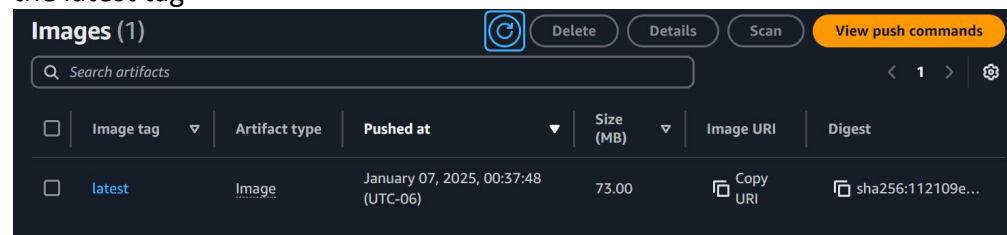


Select the registry and click on “View Push Commands”

And then run each command in the EC2 instance terminal.

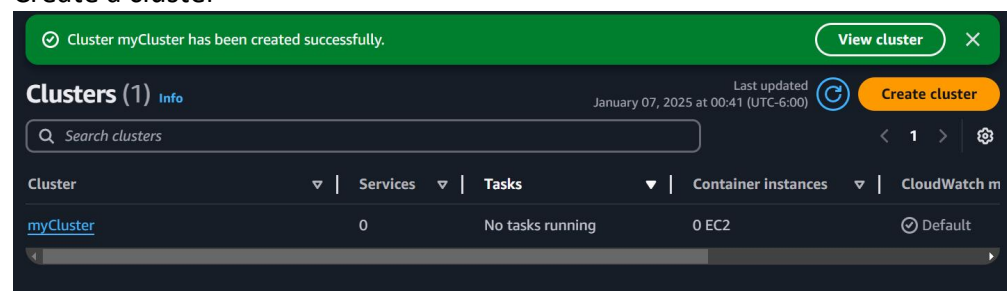
Running these commands will retrieve an authentication token and authenticate your Docker client to your registry, then build your docker image, tag your docker image so it is ready to push to the ECR repository, and finally push the docker image to ECR repository.

In AWS Console, click on the repository and you will see the image got pushed with the latest tag



Now copy image URI, and open the Elastic Container Service (ECS)

Create a cluster



Then create a task definition and select “ecsTaskExecutionRole” in Task Role

The screenshot shows the 'Task definition configuration' page in the AWS IAM console. It includes sections for 'Task definition family' (with a text input 'myDef'), 'Infrastructure requirements' (with 'Launch type' set to 'AWS Fargate'), 'OS, Architecture, Network mode' (with 'Operating system/Architecture' set to 'Linux/X86_64' and 'Network mode' set to 'awsvpc'), 'Task size' (with 'CPU' set to '1 vCPU' and 'Memory' set to '3 GB'), and 'Task roles' (with 'Task role' and 'Task execution role' both set to 'ecsTaskExecutionRole').

In the essential container, paste the image URI that we copied in the preceding step
Be sure to enter the correct port number in the container port

The screenshot shows the 'Container - 1' configuration page in the AWS IAM console. It includes sections for 'Container details' (with 'Name' set to 'htmlcontainer', 'Image URI' set to '692859948282.dkr.ecr.us-east-1.amazonaws.com/docker-stator', and 'Essential container' set to 'Yes'), 'Private registry' (with 'Private registry authentication' set to 'Off'), 'Port mappings' (with 'Container port' set to '80', 'Protocol' set to 'TCP', 'Port name' set to 'container-port-prot', and 'App protocol' set to 'HTTP'), and 'Read only root file system' (with 'Read only' set to 'Off').

Once the task is created, go back to clusters, select the cluster, go to tasks tab, and select “Run new task”

Services

Tasks

Infrastructure

Metrics

Scheduled tasks

Tags

Tasks (0)

Manage tags

Stop

Run new task

Filter tasks by property or value

Filter desired status

Filter launch type

Any desired status

Any launch type

Task

Last status

Desired st...

T...

Health sta...

Started by

Star

No tasks

No tasks to display.

Run new task

Existing cluster

myCluster

▼ Compute configuration (advanced)

Compute options

Info

To ensure task distribution across your compute types, use appropriate compute options.

Capacity provider strategy

Specify a launch strategy to distribute your tasks across one or more capacity providers.

Launch type

Launch tasks directly without the use of a capacity provider strategy.

Launch type

Info

Select either managed capacity (Fargate), or custom capacity (EC2 or user-managed, External instances). External instances are registered to your cluster using the ECS Anywhere capability.

FARGATE

Platform version

Info

Specify the platform version on which to run your service.

LATEST

Deployment configuration

Application type

Info

Specify what type of application you want to run.

Service

Launch a group of tasks handling a long-running computing work that can be stopped and restarted. For example, a web application.

Task

Launch a standalone task that runs and terminates. For example, a batch job.

Task definition

Select an existing task definition. To create a new task definition, go to [Task definitions](#).

Specify the revision manually

Manually input the revision instead of choosing from the 100 most recent revisions for the selected task definition family.

Family

Revision

myDef

1 (LATEST)

Desired tasks

Specify the number of tasks to launch.

1

In the Networking section, create a custom security group with following configuration

Security group

Info

Choose an existing security group or create a new security group.

Use an existing security group

Create a new security group

Security group details

Specify the configuration to use when creating the new security group.

Security group name

Security group description

ecs-m0m5z96a

Created in ECS Console

Security group name must be 1 to 255 characters. Valid characters are a-z, A-Z, 0-9, underscores (_), hyphens (-), colons (:), forward slashes (/), parentheses (()), hashtags (#), commas (,), at signs (@), brackets ([]), plus signs (+), equal signs (=), ampersands (&), semicolons (;), brackets ({}), exclamation points (!), dollar signs (\$), asterisks (*).

Security group description must be 1 to 255 characters. Valid characters are a-z, A-Z, 0-9, underscores (_), hyphens (-), colons (:), forward slashes (/), parentheses (()), hashtags (#), commas (,), at signs (@), brackets ([]), plus signs (+), equal signs (=), ampersands (&), semicolons (;), brackets ({}), exclamation points (!), dollar signs (\$), asterisks (*).

Inbound rules for security groups

Add one or more ingress rules for your security group.

Type

Protocol

Port range

Source

Values

HTTP

TCP

80

Anywhere

0.0.0.0/0, ::/0

Add rule

Delete

Once the task is running, click on the running task and locate the Public IP Address in the configuration. Open address, and you should be able to see your application there

← → ↻ ⚠ Not secure 44.222.63.57/test.html

Welcome to My Website

This is a test HTML page which I will be using in my projects.