

Auto Assign Elastic IP to EC2 Machine

Auto Assign Elastic IP to EC2 Machine

Steps to auto assign elastic IP to EC2 machine

1. Create IAM Role
2. Create AMI
3. Create launch Configuration
4. Create Auto Scaling Group

1. Create IAM Role

To create the IAM Role, login to AWS Console, navigate to IAM, select the Roles, to create the new role. Click on the button 'Create new role' as below screens.

Identity and Access Management (IAM)

▼ AWS Account (87665333959)

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

Q Search IAM

Welcome to Identity and Access Management

IAM users sign-in link:

..aws.amazon.com/console

IAM Resources

Users: 2 Roles: 15

Groups: 4 Identity Providers: 0

Customer Managed Policies: 2

Security Status

- ⚠ Activate MFA on your root account
- ✅ Create individual IAM users
- ✅ Use groups to assign permissions

Create role

Select type of trusted entity

- AWS service**
EC2, Lambda and others
- Another AWS account
Belonging to you or 3rd party
- Web identity
Cognito or any OpenID provider
- SAML 2.0 federation
Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose the service that will use this role

EC2

Allows EC2 instances to call AWS services on your behalf.

Lambda

Allows Lambda functions to call AWS services on your behalf.

API Gateway	Comprehend	EMR	Kinesis	S3
AWS Backup	Config	ElastiCache	Lambda	SMS

Select the AWS service and EC2 options to give access to the role and click on the button 'Next permissions' to add either existing policy or created policy as below

Create role

1 2 3 4

Review

Provide the required information below and review this role before you create it.

Role name*
Use alphanumeric and '+', '@', '-' characters. Maximum 64 characters.

Role description
Maximum 1000 characters. Use alphanumeric and '+', '@', '-' characters.

Trusted entities AWS service: ec2.amazonaws.com

Policies Policies not attached

Permissions boundary Permissions boundary is not set

No tags were added.

* Required

Cancel

Previous

Create role

1. Create AMI

To create the AMI login to AWS Console, navigate to instances, select the required instance and create the AMI from the actions as below.

Create Image

Instance ID ⓘ I-000aec4e08e7cfb1e

Image name ⓘ

Image description ⓘ

No reboot ⓘ ☐

Instance Volumes

Volume Type ⓘ	Device ⓘ	Snapshot ⓘ	Size (GiB) ⓘ	Volume Type ⓘ	IOPS ⓘ	Throughput (MB/s) ⓘ	Delete on Termination ⓘ	Encrypted ⓘ
Root	/dev/xvda	snap-03579e9b886d728d9	<input type="text" value="50"/>	General Purpose SSD (gp2) ▾	150 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Add New Volume

Total size of EBS Volumes: 50 GiB

When you create an EBS image, an EBS snapshot will also be created for each of the above volumes.

Cancel

Create Image

Click on create button to get the latest image.

3. Create Launch Configuration

To create the launch configuration follow the steps as below

Goto EC2 service and navigate to launch configuration option and click on the Create launch configuration button

AUTO SCALING

Launch Configurations

Auto Scaling Groups

[Create launch configuration](#)[Create Auto Scaling group](#)[Copy to launch template](#)[Actions](#) ▼

Filter:

☐ Name ▲ AMI ID ▼ Instance Type ▼ Spot Price ▼ Creation Time ▼

1. Choose AMI 2. Choose Instance Type 3. Configure details 4. Add Storage 5. Configure Security Group 6. Review

Create Launch Configuration

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch an instance. You can select one of your own AMIs.

[Quick Start](#)[My AMIs](#)[AWS Marketplace](#)[Community AMIs](#)

TestAS - ami-080b82d6f2ec54da1

TestForAS

Root device type: ebs Virtualization type: hvm Owner: 876653333959

1. Choose AMI 2. Choose Instance Type 3. Configure details 4. Add Storage 5. Configure Security Group 6. Review

Create Launch Configuration

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run your applications. You can choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your needs.

Filter by: [All instance types](#) [Current generation](#) [Show/Hide Columns](#)

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)



T2 instances are VPC-only. Your T2 instance will launch into your VPC. [Learn more](#) about T2 and VPC.

	Family ▼	Type ▼	vCPUs ⓘ ▼	Memory (GiB) ▼
<input type="checkbox"/>	General purpose	t2.nano	1	0.5
<input checked="" type="checkbox"/>	General purpose	t2.micro Free tier eligible	1	1

While configuring the details, select the Role as shown below, and attach the script as given below.

Create Launch Configuration

Name ⓘ

Purchasing option ⓘ ☐ Request Spot Instances

IAM role ⓘ MANAAGEEIP ▼

Monitoring ⓘ ☐ Enable CloudWatch detailed monitoring
[Learn more](#)

▼ Advanced Details

Kernel ID ⓘ ▼

RAM Disk ID ⓘ ▼

User data ⓘ ☒ As text ☐ As file ☐ Input is already base64 encoded

(Optional)

IP Address Type ⓘ ☒ Only assign a public IP address to instances launched in the default VPC and subnet. (default)
☐ Assign a public IP address to every instance.
☐ Do not assign a public IP address to any instances.
 Note: this option only affects instances launched into an Amazon VPC

Keep the below script in user data box and move to the Add storage step `#!/bin/bash`

```
INSTANCEID=$(ec2metadata --instance-id)
IPADDRESS=$(aws ec2 describe-addresses --region eu-west-1 --filters "Name=tag:instance,Values=not" | grep "PublicIp" | tail -n1 | cut -d'"' -f 4)
EIPALLOC=$(aws ec2 describe-addresses --region eu-west-1 --filters "Name=public-ip,Values=$IPADDRESS" | grep 'AllocationId' | cut -d'"' -f 4)
aws ec2 associate-address --region eu-west-1 --instance-id $INSTANCEID --allocation-id $EIPALLOC
EIPALLOCGOT=$(aws ec2 describe-addresses --region eu-west-1 --filter "Name=instance-id,Values=${INSTANCEID}" | grep 'AllocationId' | cut -d'"' -f 4)
aws ec2 create-tags --region eu-west-1 --resources $EIPALLOCGOT --tags Key=instance,Value="yes"
```

Create Launch Configuration

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store v edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store v <https://docs.aws.amazon.com/console/ec2/launchinstance/storage> about storage options in Amazon EC2.

Volume Type ⓘ	Device ⓘ	Snapshot ⓘ	Size (GiB) ⓘ	Volume Type ⓘ
Root	/dev/sda1	snap-0e601f5f49a3a3dfb	<input type="text" value="15"/>	<input type="text" value="Magnetic"/> ▼

[Add New Volume](#)

Create a 'new security group', either create a new one or else select an existing security group and review the configuration and choose the Key Pair or Create New Key Pair, select the key and click on 'Create Launch Configuration'

Create Launch Configuration

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 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

Assign a security group: ☒ Create a **new** security group
☐ Select an **existing** security group

Security group name:

Description:

Type <small>i</small>	Protocol <small>i</small>	Port Range <small>i</small>
SSH	TCP	22

Add Rule

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.

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](#).

Select a key pair

☐ I acknowledge that I have access to the selected private key file (Test.pem), and that without this file, I won't be able to log into my instance.

Cancel

Create launch configuration

Launch configuration creation status



Successfully created launch configuration: test

[View creation log](#)

View

[View your launch configurations](#)

[View your Auto Scaling groups](#)

Here are some helpful resources to get you started

4. Create Auto Scaling Group

To create the Auto Scaling Group, go to the EC2 service and navigate to the Auto Scaling Groups,

AUTO SCALING

Launch
Configurations


Auto Scaling Groups

Click on 'Create Auto Scaling Group' button and choose the launch configuration, and click on the button 'Next Step'

Create Auto Scaling Group

Complete this wizard to create your Auto Scaling group. First, choose either a launch configuration or a launch template. The Auto Scaling group uses to launch instances.

Launch Configuration

You can continue to use your launch configurations if they support the Amazon EC2 features you need. [Learn more](#) 

[Create a new launch configuration](#)

 Filter launch configurations... 

Name

AMI ID




test

ami-080b82d6f2ec54da1


Configure the Auto Scaling Group details

1. Configure Auto Scaling group details 2. Configure scaling policies 3. Configure Notifications 4. Configure Tags 5. Review

Create Auto Scaling Group

Group name 

Test_ASG

Launch Configuration 

test

Group size 


Start with instances

Network 

Launch into EC2-Classical



Create new VPC

Availability Zone(s) 


us-east-1a x us-east-1b x us-east-1c x
us-east-1d x
us-east-1e
us-east-1f

Advanced Details

Load Balancing 

☐ Receive traffic from one or more load balancers

[Learn about Elastic Load Balancing](#)

Health Check Grace Period 

seconds

Monitoring 

Amazon EC2 Detailed Monitoring metrics, which are provided at 1 minute frequency, are not enabled for the launch configuration test. Instances launched from it will use Basic Monitoring metrics, provided at 5 minute frequency.

[Learn more](#)

Instance Protection 

Service-Linked Role 

AWSServiceRoleForAutoScaling



View Role in IAM

You can optionally add scaling policies if you want to adjust the size (number of instances) of your group automatically. A scaling policy is a set of instructions for making such adjustments in response to an Amazon CloudWatch alarm that you assign to it. In each policy, you can choose to add or

remove a specific number of instances or a percentage of the existing group size, or you can set the group to an exact size. When the alarm triggers, it will execute the policy and adjust the size of your group accordingly.

- ☒ **Keep this group at its initial size**
- ☐ **Use scaling policies to adjust the capacity of this group**

Configure your Auto Scaling group to send notifications to a specified endpoint, such as an email address, whenever a specified event takes place, including: successful launch of an instance, failed instance launch, instance termination, and failed instance termination. If you created a new topic, check your email for a confirmation message and click the included link to confirm your subscription. Notifications can only be sent to confirmed addresses.

In the Configure Tags screen, create the Tag & Value and Review the configurations and click on the 'Create Auto Scaling Group' button.