



## Resource EC2 Instance

In this lab, the goal is to create and manage an EC2 instance using AWS CloudFormation. The process includes the following key steps:

1. **Creating an EC2 Instance:** Using a CloudFormation template, you create an EC2 instance that includes a default security group. You'll need an AMI ID and a Key Pair for this setup.
2. **Using CloudFormation Templates:** You download, unzip, and modify templates from GitHub, then upload them to create a stack in CloudFormation.
3. **Managing Security Groups:** You create a new security group and attach it to the instance using CloudFormation.
4. **Updating Security Groups:** You add new rules to the existing security group by modifying and uploading the template.
5. **Adding Elastic IP:** You associate an Elastic IP with the instance by updating the CloudFormation template.

**End Goal:** The primary objective is to automate the creation, configuration, and management of an EC2 instance using CloudFormation, demonstrating how to manage infrastructure as code, modify security settings, and allocate resources efficiently.



## To begin with the Lab

1. In this lab we are going to create an EC2 instance using cloud formation. Below you can see the code that we are going to use. Here you can see that we are including the security group, which is the default SG for now.
2. Now you can get the templates from GitHub. Download them and unzip them make changes accordingly and then use them.
3. Also, you need to have the AMI ID and the Key pair. For key pair go to EC2 and create it and for AMI ID, you can get it by browsing.

```

1 AWSTemplateFormatVersion: 2010-09-09
2 Description: Basic EC2 Instance.
3
4 Resources:
5   EC2Instance:
6     Type: AWS::EC2::Instance
7     Properties:
8       ImageId: ami-0e97ea97a2f374e3d
9       InstanceType: t2.micro
10      KeyName: CFKeyPair
11      SecurityGroups:
12        - default

```

4. Now in your AWS Console you need to navigate to cloud formation and then you need to create a stack.
5. Then you need to click on choose an existing template then we need to choose to upload a template file. After that browse into your system and upload the template.

Create stack

**Prerequisite - Prepare template**

Prepare template  
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

Choose an existing template  
Upload or choose an existing template.

Use a sample template  
Choose from our sample template library.

Build from Application Composer  
Create a template using a visual builder.

**Specify template Info**  
A template is a JSON or YAML file that describes your stack's resources and properties.

Template source  
Selecting a template generates an Amazon S3 URL where it will be stored.

Amazon S3 URL  
Provide an Amazon S3 URL to your template.

Upload a template file  
Upload your template directly to the console.

Sync from Git - new  
Sync a template from your Git repository.

Upload a template file

6. Now you need to give your stack a name then moves to the review page and create your stack.

## Specify stack details

Provide a stack name

Stack name

Stack name must be 1 to 128 characters, start with a letter, and only contain alphanumeric characters. Character count: 9/128.

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

No parameters

There are no parameters defined in your template

[Cancel](#) [Previous](#) [Next](#)

7. Now if you go to the Events section then you will see the events which can help you to visualize the process scenarios.

Stack-EC2								
Stack info		Events		Resources				
Stack info		Events		Resources	Outputs	Parameters		
Stack info		Events		Template	Change sets	Git sync - new		
<strong>Events (7)</strong>								
<input type="text"/> Search events								
Timestamp	Logical ID	Status	Detailed status	Status reason				
2024-07-18 13:08:59 UTC+0530	Stack-EC2	CREATE_COMPLETE	-	-				
2024-07-18 13:08:58 UTC+0530	EC2Instance	CREATE_COMPLETE	-	-				
2024-07-18 13:08:38 UTC+0530	Stack-EC2	CREATE_IN_PROGRESS	CONFIGURATION_COMPLETE	Eventual consistency check initiated				
2024-07-18 13:08:38 UTC+0530	EC2Instance	CREATE_IN_PROGRESS	CONFIGURATION_COMPLETE	Eventual consistency check initiated				
2024-07-18 13:08:27 UTC+0530	EC2Instance	CREATE_IN_PROGRESS	-	Resource creation Initiated				
2024-07-18 13:08:25 UTC+0530	EC2Instance	CREATE_IN_PROGRESS	-	-				
2024-07-18 13:08:23 UTC+0530	Stack-EC2	CREATE_IN_PROGRESS	-	User Initiated				

8. Also, navigate to EC2 and here you will see that our instance has been created. You can check for the key pair.

**Instances (1/1) Info**

Find Instance by attribute or tag (case-sensitive)

Instance state: running | All states

Launch instances

Instance state | Instance ID | Instance state | Instance type | Status check | Alarm status

i-079a7a1edc3a1d7c6 | Running | t2.micro | 2/2 checks passed | View alarms +

**i-079a7a1edc3a1d7c6**

Details | Status and alarms | Monitoring | Security | Networking | Storage | Tags

Instance summary

Instance ID: i-079a7a1edc3a1d7c6

IPv6 address: -

Hostname type: IP name: ip-172-31-24-250.ap-southeast-1.compute.internal

Public IPv4 address: 18.141.201.192 | open address

Instance state: Running

Private IP DNS name (IPv4 only): ip-172-31-24-250.ap-southeast-1.compute.internal

Private IPv4 addresses: 172.31.24.250

Public IPv4 address: ec2-18-141-201-192.ap-southeast-1.compute.amazonaws.com | open address

9. Now in the security you will see your security group attached to your instance.

**i-079a7a1edc3a1d7c6**

Details | Status and alarms | Monitoring | **Security** | Networking | Storage | Tags

Security details

IAM Role: -

Owner ID: 878893308172

Security groups:

sg-09db77cb9950792bc (default)

10. Also, you can view the different tags assigned to your instance.

**i-079a7a1edc3a1d7c6**

Details | Status and alarms | Monitoring | Security | Networking | Storage | **Tags**

Tags

Manage tags

Key	Value
aws:cloudformation:logical-id	EC2Instance
aws:cloudformation:stack-name	Stack-EC2
aws:cloudformation:stack-id	arn:aws:cloudformation:ap-southeast-1:878893308172:stack/Stack-EC2/b6879be0-44d8-11ef-9fef-0a4a71e97fb3

11. Now if you click on connect and choose EC2 instance connect and try to connect your instance you will see that your instance was successfully connected.



**Instances (1/1) Info**

Instance state = running		Clear filters	Actions	Launch instances
<input checked="" type="checkbox"/>	Name <input type="text" value="i-079a7a1edc3a1d7c6"/>	Instance ID <input type="text" value="i-079a7a1edc3a1d7c6"/>	Instance state <input checked="" type="radio"/> Running	Instance type t2.micro
			Status check <input checked="" type="radio"/> 2/2 checks passed	View alarm

**EC2 Instance Connect**

- [Session Manager](#)
- [SSH client](#)
- [EC2 serial console](#)

Instance ID:

Connection Type:

- Connect using EC2 Instance Connect  
Connect using the EC2 Instance Connect browser-based client, with a public IPv4 address.
- Connect using EC2 Instance Connect Endpoint  
Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

Public IP address:

Username:

**Note:** In most cases, the default username, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

**Cancel** **Connect**

i-079a7a1edc3a1d7c6  
PublicIPs: 18.141.201.192 PrivateIPs: 172.31.24.250

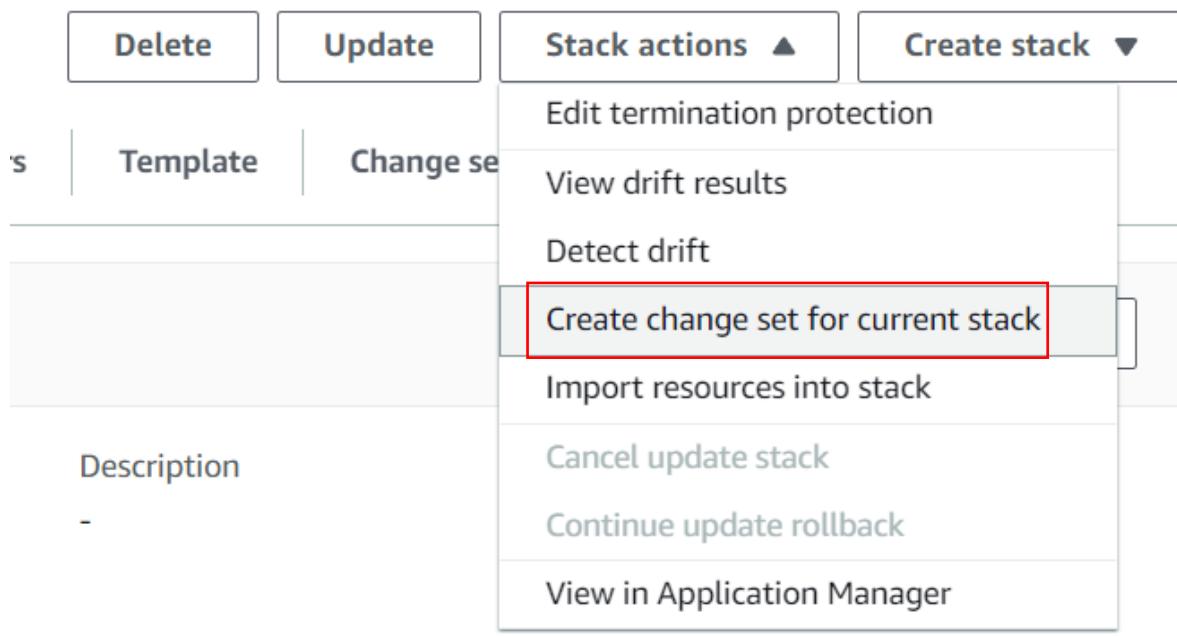
© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

## 😊 Security Group

1. Now we will create a new security group for our instance and attach it. Below you can see that code that we are using in our template.

```
1 AWSTemplateFormatVersion: 2010-09-09
2 Description: Basic EC2 Instance.
3
4 Resources:
5   EC2Instance:
6     Type: AWS::EC2::Instance
7     Properties:
8       ImageId: ami-0e97ea97a2f374e3d
9       InstanceType: t2.micro
10      KeyName: CFKeyPair
11      SecurityGroups:
12        - default
13        - !Ref SSHSecurityGroup
14
15      SSHSecurityGroup:
16        Type: AWS::EC2::SecurityGroup
17        Properties:
18          GroupDescription: my new SSH SG
19          SecurityGroupIngress:
20            - IpProtocol: tcp
21              FromPort: '22'
22              ToPort: '22'
23              CidrIp: 0.0.0.0/0
24
```

2. So, now in your cloud formation you need to expand stack actions and choose to create a change set for the current stack.



3. And again, we need to replace it with the existing template and then upload our template.
4. After that just move to the review page and click on submit.

### Create change set for Stack1Creating-EC2-Instance

**Prerequisite - Prepare template**

Prepare template  
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

Use existing template  
Proceed with the template you are already using for this stack.

Replace existing template  
Replace your existing template with a new template.

Edit in Application Composer  
Edit your template in a visual builder.

**Specify template**  
A template is a JSON or YAML file that describes your stack's resources and properties.

Template source  
Selecting a template generates an Amazon S3 URL where it will be stored.

Amazon S3 URL

Upload a template file

5. Now you will see that your change set has been created and now you have the ability to execute this change set.
6. If you want to execute then click on execute or else, you can delete this change set.
7. Now just click on execute change set. Also, you can see that there are a total of two changes.

CloudFormation > Stacks > Stack-EC2 > Change sets: Stack-EC2-nsim9m21jr-fa5r0emkngd

### Stack-EC2-nsim9m21jr-fa5r0emkngd

**Overview**

Change set ID arn:aws:cloudformation:ap-southeast-1:878893308172:changeSet/Stack-EC2-nsim9m21jr-fa5r0emkngd/ef58fc2-21db-47c9-8b5f-9ac08ff6212e	Status <span style="color: green;">CREATE_COMPLETE</span>
Description Basic EC2 Instance.	Status reason -
Created time 2024-07-18 14:26:17 UTC+0530	Execution status <span style="color: green;">AVAILABLE</span>

**Changes** | Input | Template | JSON changes | Hook invocations

**Changes (2)**

Preview how proposed changes to a stack will impact running resources. Click on "View details" to preview the impact on property values for a resource.

Action	Logical ID	Resource type	Replacement	Property-level changes	Policy action	Physical ID	Module	Hook invocations
<span style="background-color: #00A0C0; color: white; padding: 2px 5px;">Modify</span>	EC2Instance	AWS::EC2::Instance	True	<a href="#">View details</a>	<span style="background-color: #E67E22; color: white; padding: 2px 5px;">ReplaceAndDelete</span>	i-079a7a1edc3a1d7c6	-	-
<span style="background-color: #00A0C0; color: white; padding: 2px 5px;">Add</span>	SSHSecurityGroup	AWS::EC2::SecurityGroup	True	<a href="#">View details</a>	-	-	-	-

8. Then go to the events to see the real-time progress and below you can see the process.

Stack info | **Events** | Resources | Outputs | Parameters | Template | Change sets | Git sync - new

**Events (18)**

Q Search events

Timestamp	Logical ID	Status	Detailed status	Status reason
2024-07-18 14:33:55 UTC+0530	Stack-EC2	<span style="color: green;">UPDATE_COMPLETE</span>	-	-
2024-07-18 14:33:55 UTC+0530	EC2Instance	<span style="color: green;">DELETE_COMPLETE</span>	-	-
2024-07-18 14:33:22 UTC+0530	EC2Instance	<span style="color: blue;">DELETE_IN_PROGRESS</span>	-	-
2024-07-18 14:33:21 UTC+0530	Stack-EC2	<span style="color: blue;">UPDATE_COMPLETE_CLEANUP_IN_PROGRESS</span>	-	-
2024-07-18 14:33:20 UTC+0530	EC2Instance	<span style="color: green;">UPDATE_COMPLETE</span>	-	-
2024-07-18 14:32:49 UTC+0530	EC2Instance	<span style="color: blue;">UPDATE_IN_PROGRESS</span>	-	Resource creation Initiated
2024-07-18 14:32:47 UTC+0530	EC2Instance	<span style="color: blue;">UPDATE_IN_PROGRESS</span>	-	Requested update requires the creation of a new physical resource, hence creating one.
2024-07-18 14:32:45 UTC+0530	SSHSecurityGroup	<span style="color: green;">CREATE_COMPLETE</span>	-	-
2024-07-18 14:32:45 UTC+0530	SSHSecurityGroup	<span style="color: blue;">CREATE_IN_PROGRESS</span>	-	Resource creation Initiated
2024-07-18 14:32:42 UTC+0530	SSHSecurityGroup	<span style="color: blue;">CREATE_IN_PROGRESS</span>	-	-
2024-07-18 14:32:40 UTC+0530	Stack-EC2	<span style="color: blue;">UPDATE_IN_PROGRESS</span>	-	User Initiated

9. Now go to EC2, here you will see that our previous instance was terminated and the new instance was created.

Instances (2) Info

Q Find Instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
	i-079a7a1edc3a1d7c6	Terminated	t2.micro	-	<a href="#">View alarms</a> +	ap-southeast-1a
	i-004835842cde0ef7b	Running	t2.micro	<span style="color: green;">2/2 checks passed</span>	<a href="#">View alarms</a> +	ap-southeast-1a

10. In your new instance if you go to the security tab you will see two security groups also you can log in to your instance through the Putty application.

Instances (1/2) [Info](#)

Find Instance by attribute or tag (case-sensitive)

All states ▾

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
	i-079a7a1edc3a1d7c6	Terminated	t2.micro	-	<a href="#">View alarms</a> +	ap-southeast-1a
<input checked="" type="checkbox"/>	i-004835842cde0ef7b	Running	t2.micro	2/2 checks passed	<a href="#">View alarms</a> +	ap-southeast-1a

i-004835842cde0ef7b

Details | Status and alarms | Monitoring | **Security** | Networking | Storage | Tags

▼ Security details

IAM Role -

Owner ID 878893308172

Launch time Thu Jul 18 2024 14:32:48 GMT+0530 (India Standard Time)

Security groups

sg-074ab890fb7e218cb (Stack-EC2-SSHSecurityGroup-L1jvghsKL15Y)  
sg-09db77cb950792bc (default)

## 😊 Adding a new rule

1. Now we are going to add a new rule to our existing security group. For that, we have added some changes to our template. Below you can see that from line 23 we have introduced a new port.

```

1  AWSTemplateFormatVersion: 2010-09-09
2  Description: Basic EC2 Instance.
3
4  Resources:
5  EC2Instance:
6      Type: AWS::EC2::Instance
7  Properties:
8      ImageId: ami-0e97ea97a2f374e3d
9      InstanceType: t2.micro
10     KeyName: CFKeyPair
11  SecurityGroups:
12      - default
13      - !Ref SSHSecurityGroup
14  SSHSecurityGroup:
15      Type: AWS::EC2::SecurityGroup
16  Properties:
17      GroupDescription: my new SSH SG
18  SecurityGroupIngress:
19      - IpProtocol: tcp
20          FromPort: '22'
21          ToPort: '22'
22          CidrIp: 0.0.0.0/0
23      - IpProtocol: tcp
24          FromPort: '8080'
25          ToPort: '8080'
26          CidrIp: 0.0.0.0/0
27
28

```

2. Now again we need to go to our Cloud formation stack and choose the create change stack feature to upload our new template.

## Create change set for Stack-EC2

**Prerequisite - Prepare template**

Prepare template  
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

Use existing template  
Proceed with the template you are already using for this stack.

Replace existing template  
Replace your existing template with a new template.

Edit in Application Composer  
Edit your template in a visual builder.

**Specify template**  
A template is a JSON or YAML file that describes your stack's resources and properties.

Template source  
Selecting a template generates an Amazon S3 URL where it will be stored.

Amazon S3 URL

Upload a template file

Upload a template file

3. This time you can see that there is only one change that will occur.

CloudFormation > Stacks > Stack-EC2 > Change sets: Stack-EC2-oe5kqq5apeq-g13ysyhrgu

Stack-EC2-oe5kqq5apeq-g13ysyhrgu Delete change set Execute change set

**Overview**

Change set ID arn:aws:cloudformation:ap-southeast-1:878893308172:changeSet/Stack-EC2-oe5kqq5apeq-g13ysyhrgu/574bc160-4c48-4c13-b352-e21eb1984c98	Status <span>CREATE_COMPLETE</span>
Description Basic EC2 Instance.	Status reason -
Created time 2024-07-18 14:43:25 UTC+0530	Execution status <span>AVAILABLE</span>

**Changes** | Input | Template | JSON changes | Hook invocations

**Changes (1)**  
Preview how proposed changes to a stack will impact running resources. Click on "View details" to preview the impact on property values for a resource.

Action	Logical ID	Resource type	Replacement	Property-level changes	Policy action	Physical ID	Module
Modify	SSHSecurityGroup	AWS::EC2::SecurityGroup	False	<a href="#">View details</a>	-	Stack-EC2-SSHSecuri...	-

4. Now in the events tab you can see that our update has been initiated now if we go to our security group we will see the added inbound rule.

Stack Info | **Events** | Resources | Outputs | Parameters | Template | Change sets | Git sync - new

**Events (23)**

Timestamp	Logical ID	Status	Detailed status	Status reason
2024-07-18 14:59:37 UTC+0530	Stack-EC2	<span>UPDATE_COMPLETE</span>	-	-
2024-07-18 14:59:36 UTC+0530	Stack-EC2	<span>UPDATE_COMPLETE_CLEANUP_IN_PROGRESS</span>	-	-
2024-07-18 14:59:35 UTC+0530	SSHSecurityGroup	<span>UPDATE_COMPLETE</span>	-	-
2024-07-18 14:59:34 UTC+0530	SSHSecurityGroup	<span>UPDATE_IN_PROGRESS</span>	-	-
2024-07-18 14:59:31 UTC+0530	Stack-EC2	<span>UPDATE_IN_PROGRESS</span>	-	User Initiated

5. Below we can see that the port has been added successfully.

EC2 > Security Groups > sg-074ab890fb7e218cb - Stack-EC2-SSHSecurityGroup-L1jvghsKLI5Y

sg-074ab890fb7e218cb - Stack-EC2-SSHSecurityGroup-L1jvghsKLI5Y Actions ▾

Details			
Security group name Stack-EC2-SSHSecurityGroup-L1jvghsKLI5Y	Security group ID sg-074ab890fb7e218cb	Description my new SSH SG	VPC ID vpc-0c438557fe24ea59e
Owner 878893308172	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry	

Inbound rules | Outbound rules | Tags

Inbound rules (2)

<input type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol	Port range	Source
<input type="checkbox"/>	-	sgr-0962567c01573b...	IPv4	SSH	TCP	22	0.0.0.0/0
<input type="checkbox"/>	-	sgr-057f170a9a8278349	IPv4	Custom TCP	TCP	8080	0.0.0.0/0

## 😊 Adding Elastic IP

1. Now we are going to add an Elastic IP to our instance, for that we have our template ready. You can see the code below.

```

1 AWSTemplateFormatVersion: 2010-09-09
2 Description: Basic EC2 Instance.
3
4 Resources:
5   EC2Instance:
6     Type: AWS::EC2::Instance
7     Properties:
8       ImageId: ami-0e97ea97a2f374e3d
9       InstanceType: t2.micro
10      KeyName: CFKeyPair
11      SecurityGroups:
12        - default
13        - !Ref SSHSecurityGroup
14   SSHSecurityGroup:
15     Type: AWS::EC2::SecurityGroup
16     Properties:
17       GroupDescription: my new SSH SG
18     SecurityGroupIngress:
19       - IpProtocol: tcp
20         FromPort: '22'
21         ToPort: '22'
22         CidrIp: 0.0.0.0/0
23       - IpProtocol: tcp
24         FromPort: '8080'
25         ToPort: '8080'
26         CidrIp: 0.0.0.0/0
27
28   MyElasticIP:
29     Type: AWS::EC2::EIP
30     Properties:
31       InstanceId: !Ref EC2Instance

```

2. Now again the steps are the same just go to your stack and choose to create a change stack set for the current stack.
3. Below you can see that it is showing us the addition of our Elastic IP.

**Overview**

Change set ID arn:aws:cloudformation:ap-southeast-1:878893308172:changeSet/Stack-EC2-e0r0pxetcmd-s6mm4pp2t5q/baa2ca1b-c0a5-4c84-be9c-a2859e962f3f	Status <span style="color: green;">CREATE_COMPLETE</span>
Description Basic EC2 Instance.	Status reason -
Created time 2024-07-18 15:06:17 UTC+0550	Execution status <span style="color: green;">AVAILABLE</span>

**Changes (1)**

Preview how proposed changes to a stack will impact running resources. Click on "View details" to preview the impact on property values for a resource.

Action	Logical ID	Resource type	Replacement	Property-level changes	Policy action	Physical ID	Module
Add	MyElasticIP	AWS::EC2::EIP	True	<a href="#">View details</a>	-	-	-

#### 4. Also, in the events you can see the process.

**Events (29)**

Timestamp	Logical ID	Status	Detailed status	Status reason
2024-07-18 15:12:15 UTC+0530	Stack-EC2	<span style="color: green;">UPDATE_COMPLETE</span>	-	-
2024-07-18 15:12:14 UTC+0530	Stack-EC2	<span style="color: blue;">UPDATE_COMPLETE_CLEANUP_IN_PROGRESS</span>	-	-
2024-07-18 15:12:13 UTC+0530	MyElasticIP	<span style="color: green;">CREATE_COMPLETE</span>	-	-
2024-07-18 15:11:56 UTC+0530	MyElasticIP	<span style="color: blue;">CREATE_IN_PROGRESS</span>	-	Resource creation Initiated
2024-07-18 15:11:56 UTC+0530	MyElasticIP	<span style="color: blue;">CREATE_IN_PROGRESS</span>	-	-
2024-07-18 15:11:53 UTC+0530	Stack-EC2	<span style="color: blue;">UPDATE_IN_PROGRESS</span>	-	User Initiated

#### 5. Now go to EC2 and check whether your instance has the Elastic IP or not. First, go directly to Elastic IP and here you can see that, then go to the associated instance ID.

**Elastic IP addresses (1/1)**

Name	Allocated IPv4 address	Type	Allocation ID	Reverse DNS record	Associated instance ID
-	13.213.212.170	Public IP	eipalloc-0d92ff19d90fa623f	-	i-004835842cd0ef7b

13.213.212.170

**Summary**

Allocated IPv4 address <a href="#">13.213.212.170</a>	Type <a href="#">Public IP</a>	Allocation ID <a href="#">eipalloc-0d92ff19d90fa623f</a>	Reverse DNS record -
Association ID <a href="#">eipassoc-0aa2ea0bb3a6174b9</a>	Scope <a href="#">VPC</a>	Associated instance ID <a href="#">i-004835842cd0ef7b</a>	Private IP address <a href="#">172.31.16.118</a>
Network interface ID <a href="#">eni-0c7aa9d3c1d82a813</a>	Network interface owner account ID <a href="#">878893308172</a>	Public DNS <a href="#">ec2-13-213-212-170.ap-southeast-1.compute.amazonaws.com</a>	NAT Gateway ID -
Address pool <a href="#">Amazon</a>	Network border group <a href="#">ap-southeast-1</a>		

#### 6. And in the instance too you will see the elastic IP address.

**Instances (1/2) Info**

All states ▾

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Pu
	i-079a7a1edc3a1d7c6	Terminated	t2.micro	-	<a href="#">View alarms +</a>	ap-southeast-1a	-
<input checked="" type="checkbox"/>	i-004835842cde0ef7b	Running	t2.micro	2/2 checks passed	<a href="#">View alarms +</a>	ap-southeast-1a	ec:

**i-004835842cde0ef7b**

[Details](#) | [Status and alarms](#) | [Monitoring](#) | [Security](#) | [Networking](#) | [Storage](#) | [Tags](#)

**Instance summary** [Info](#)

Instance ID <a href="#">i-004835842cde0ef7b</a>	Public IPv4 address <a href="#">13.213.212.170 [open address]</a>	Private IPv4 addresses <a href="#">172.31.16.118</a>
IPv6 address -	Instance state <a href="#">Running</a>	Public IPv4 DNS <a href="#">ec2-13-213-212-170.ap-southeast-1.compute.amazonaws.com [open address]</a>
Hostname type IP name: ip-172-31-16-118.ap-southeast-1.compute.internal	Private IP DNS name (IPv4 only) <a href="#">ip-172-31-16-118.ap-southeast-1.compute.internal</a>	Elastic IP addresses <a href="#">13.213.212.170 [Public IP]</a>
Answer private resource DNS name -	Instance type t2.micro	AWS Compute Optimizer finding <a href="#">Opt-in to AWS Compute Optimizer for recommendations.</a>   <a href="#">Learn more</a>
Auto-assigned IP address -	VPC ID <a href="#">vpc-0c438557fe24ea59e</a>	