

[illegible]

<b>Name</b>	AWS Config
<b>URL</b>	<a href="https://attackdefense.com/challengedetails?cid=2491">https://attackdefense.com/challengedetails?cid=2491</a>
<b>Type</b>	AWS Cloud Security : Defense

**Important Note:** This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

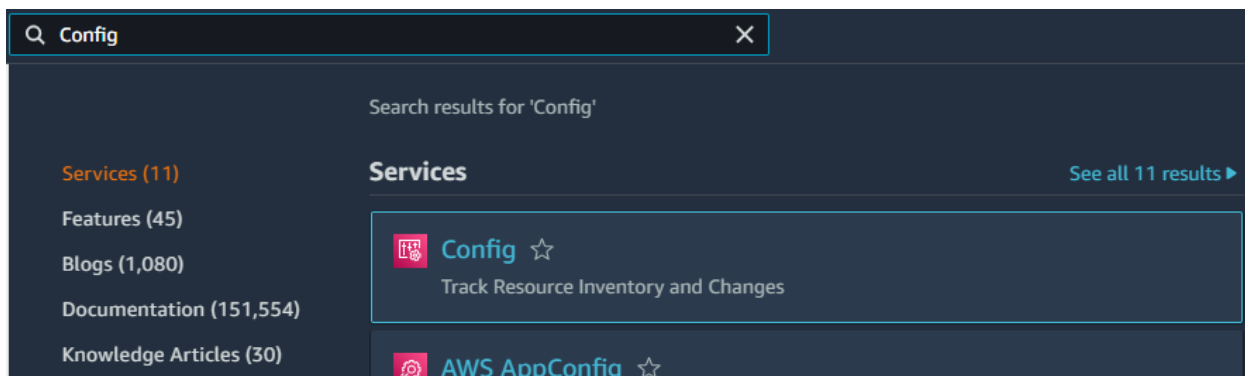
### Solution:

**Step 1:** Click the lab link button to get access credentials.

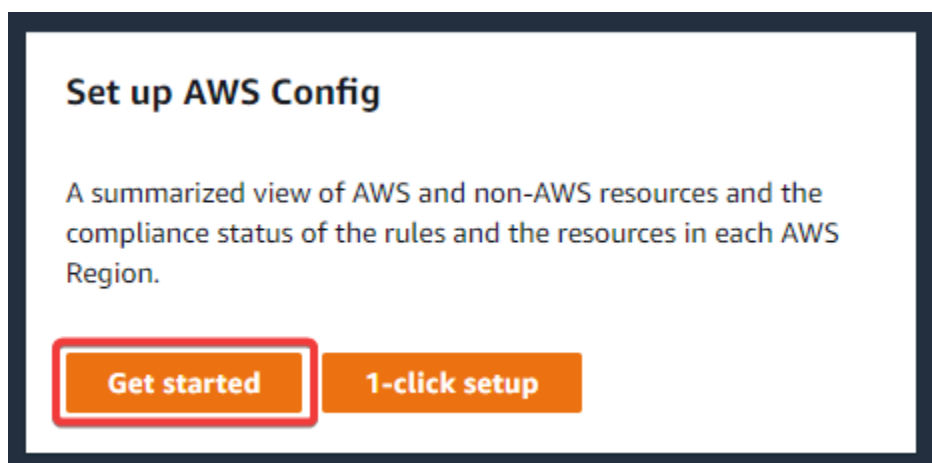
## Access Credentials to your AWS lab Account

<b>Login URL</b>	<a href="https://342103134475.signin.aws.amazon.com/console">https://342103134475.signin.aws.amazon.com/console</a>
<b>Region</b>	US East (N. Virginia) us-east-1
<b>Username</b>	student
<b>Password</b>	Ad577xOB7C8fIT0g
<b>Access Key ID</b>	AKIAU7JXPSEFQ55MA4KE
<b>Secret Access Key</b>	6VNTJUZXGhEiSKLOpJ0MBYK1J+3HjAd3zLqDeIHKh

**Step 2:** Search for Config in the search bar and navigate to the Config dashboard.



**Step 3:** Click on the “Get Started” button.



After setting up, AWS Config will evaluate your AWS resources against the rules that you chose. Additional rules can be created and existing ones can be updated and in your account after setup.

**Step 4:** Choose type to record as “Record all resources supported in this region” and set AWS Config rule as “Create AWS Config service-linked role”.

AWS Config records configuration changes for supported AWS resource types as well as third-party resource types registered in the AWS CloudFormation registry. AWS Config automatically starts recording new supported AWS resource types.

Service-linked roles are predefined by AWS Config and include all the permissions that the service requires to call other AWS services.

## Settings

### General settings

Resource types to record

☒ Record all resources supported in this region

☐ Record specific resource types

To learn more, see [Supported Resource Types](#).

☒ Include global resources (e.g., AWS IAM resources)

Supported global resource types are IAM users, groups, roles, and customer managed policies.

AWS Config role

☒ Create AWS Config service-linked role

☐ Choose a role from your account

**Step 5:** Choose “Create a bucket” and use the default bucket name.

### Delivery method

Amazon S3 bucket

☒ Create a bucket

☐ Choose a bucket from your account

☐ Choose a

Ensure appropriate permissions are available in this S3 bucket's policy. [Learn more](#).

S3 bucket name

config-bucket-342103134475

Prefix (optional)

/AWSLogs/342103134475/Config/us-east-1

Amazon SNS topic

☐ Stream configuration changes and notifications to an Amazon SNS topic.

If you choose email as the notification endpoint for your SNS topic, this can cause a high volume of email. [Learn more](#).

**Step 6:** Create a Config rule. Search for “EC2” in AWS Managed rules. Managed rules are predefined, customizable rules created by AWS Config.

## Rules

### AWS Managed Rules (154)



23 matches

<input type="checkbox"/>	Name	Labels	Description
--------------------------	------	--------	-------------

Select “ec2-imdsv2-check” and “ec2-instance-no-public-ip”..

<input type="checkbox"/>	ec2-ebs-encryption-by-default	EC2, EBS	default. The rule is NON_COMPLIANT if the encryption is not enabled.
<input checked="" type="checkbox"/>	ec2-imdsv2-check	EC2, IMDSv2, metadata	Checks whether your Amazon Elastic Compute Cloud (Amazon EC2) instance metadata version is configured with Instance Metadata Service Version 2 (IMDSv2). The rule is NON_COMPLIANT if the HttpTokens is set to optional.
<input type="checkbox"/>	ec2-instance-detailed-monitoring-enabled	EC2	Checks whether detailed monitoring is enabled for EC2 instances.
<input type="checkbox"/>	ec2-instance-managed-by-systems-manager	EC2, SystemsManager	Checks whether the Amazon EC2 instances in your account are managed by AWS Systems Manager.
<input type="checkbox"/>	ec2-instance-multiple-eni-check	EC2, Instance, ENI, EFA, Network, Interface	Checks if Amazon Elastic Compute Cloud (Amazon EC2) uses multiple ENIs (Elastic Network Interfaces) or Elastic Fabric Adapters (EFAs). This rule is NON_COMPLIANT an Amazon EC2 instance use multiple network interfaces.
<input checked="" type="checkbox"/>	ec2-instance-no-public-ip	EC2, PublicIP, Instance	Checks whether Amazon Elastic Compute Cloud (Amazon EC2) instances have a public IP association. The rule is NON_COMPLIANT if the publicIp field is present in the Amazon EC2 instance configuration item. This rule applies only to IPv4.

Cancel Previous Next

Select “ec2-instance-profile-attached” and scroll to the bottom.

AWS Managed Rules (154)			
<input type="text" value="EC2"/>		X	23 matches < 1 2 3 > ⚙
<input type="checkbox"/>	Name	Labels	Description
<input checked="" type="checkbox"/>	ec2-instance-profile-attached	EC2, INSTANCE, PROFILE	Checks if an Amazon Elastic Compute Cloud (Amazon EC2) instance has an Identity and Access Management (IAM) profile attached to it. This rule is NON_COMPLIANT if no IAM profile is attached to the Amazon EC2 instance.
<input type="checkbox"/>	ec2-instances-in-vpc	EC2	Checks whether your EC2 instances belong to a virtual private cloud (VPC).
<input type="checkbox"/>		SystemsManager,	Checks whether the compliance status of the AWS Systems Manager association compliance is COMPLIANT or

Select “ec2-volume-inuse-check” and “restricted-ssh”.

<input type="checkbox"/>	ec2-stopped-instance	EC2	allowed number of days.
<input checked="" type="checkbox"/>	ec2-volume-inuse-check	EC2	Checks whether EBS volumes are attached to EC2 instances.
<input type="checkbox"/>	eip-attached	EC2	Checks whether all EIP addresses allocated to a VPC are attached to EC2 instances or in-use ENIs.
<input type="checkbox"/>	encrypted-volumes	EC2	Checks whether EBS volumes that are in an attached state are encrypted.
<input checked="" type="checkbox"/>	restricted-ssh	EC2	Checks whether security groups that are in use disallow unrestricted incoming SSH traffic.

Cancel Previous Next

**Step 7:** Review the Config setup.

## Review

Review your AWS Config setup details. You can go back to edit changes for each section. Choose **Confirm** to finish setting up AWS Config.

### General settings

Resource types to record  
All resources (including global resources)

AWS Config role  
AWSServiceRoleForConfig

### Delivery method

S3 bucket name  
config-bucket-342103134475

### ▼ AWS Config rules (5)

ec2-instance-profile-attached  
ec2-volume-inuse-check  
restricted-ssh  
ec2-instance-no-public-ip  
ec2-imdsv2-check

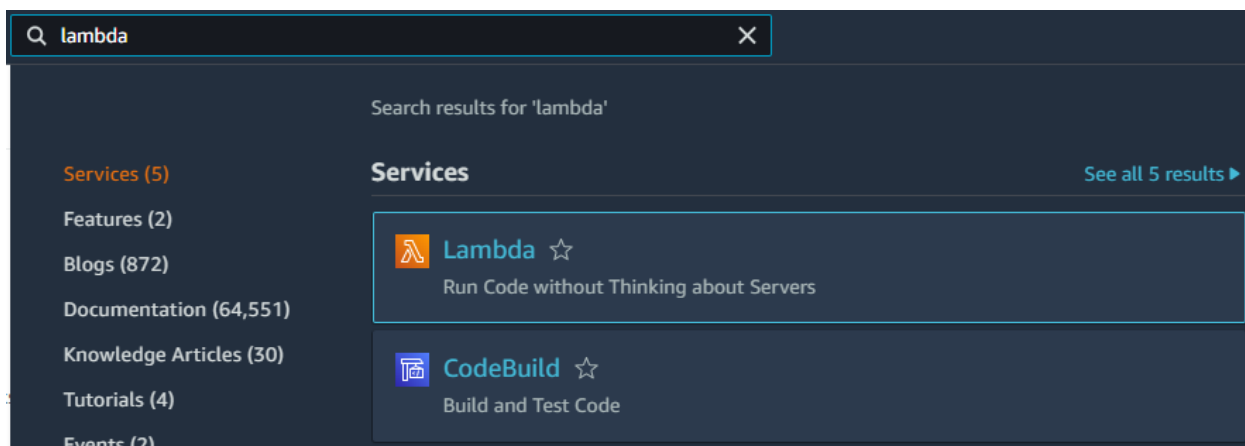
**Step 8:** Click on Confirm.

Cancel Previous Confirm

Now create a custom rule using lambda. To create this rule, first, you will create an AWS Lambda function by customizing a blueprint in the AWS Lambda console. Then, you will create a Custom Lambda rule in AWS Config, and you will associate the rule with the function.

**Step 9:** Search for “lambda” in the search bar and navigate to the Lambda dashboard.





**Step 10:** Click on the “Create function” button.



**Step 11:** Choose “Use a blueprint” and search for “config” in the blueprints filter and select “Config rule triggered by EC2 configuration change”.



## Create function [Info](#)

Choose one of the following options to create your function.

### Author from scratch ☐

Start with a simple Hello World example.

### Use a blueprint ☒

Build a Lambda application from sample code and configuration presets for common use cases.

## Blueprints (1/49) [Info](#)

Matches: 2

config



Clear filters

### Config rule triggered by EC2 configuration change ☒

An AWS Config rule that is triggered by configuration changes to EC2 instances. Checks instance types.

nodejs · config

### Config rule triggered periodically ☐

An AWS Config rule that is triggered periodically. Checks for a maximum number of resources in your account.

nodejs · config

**Step 12:** Set function name as “ec2-config-change” and choose “Create a new role from AWS policy templates” as execution role and set role name as “ec2-config-change-role”. Use the default policy for policy templates.


## Basic information [Info](#)

Function name

Execution role

Choose a role that defines the permissions of your function. To create a custom role, go to the [IAM console](#).

- ☐ Create a new role with basic Lambda permissions
- ☐ Use an existing role
- ☒ Create a new role from AWS policy templates

 Role creation might take a few minutes. Please do not delete the role or edit the trust or permission in this role.

Role name


Enter a name for your new role.

Use only letters, numbers, hyphens, or underscores with no spaces.

Policy templates - *optional* [Info](#)

Choose one or more policy templates.



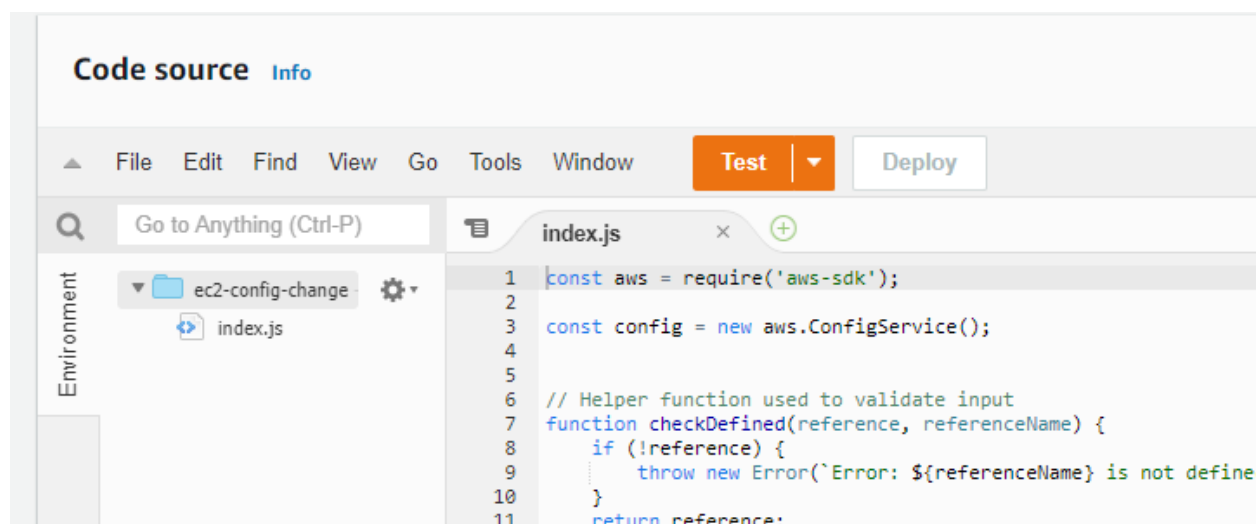
AWS Config Rules permissions   
Config S3

**Step 13:** Click on the “Create function” button.

Cancel

Create function

**Step 14:** Check out the source code in index.js file. Here you can customize the code according to your need.



**Code source** [Info](#)

File Edit Find View Go Tools Window **Test** [Deploy](#)

Go to Anything (Ctrl-P)

Environment


- ec2-config-change
  - index.js

```
1 const aws = require('aws-sdk');
2
3 const config = new aws.ConfigService();
4
5 // Helper function used to validate input
6 function checkDefined(reference, referenceName) {
7   if (!reference) {
8     throw new Error(`Error: ${referenceName} is not define
9   }
10 }
11 return reference;
```

**Step 15:** Copy the function ARN.

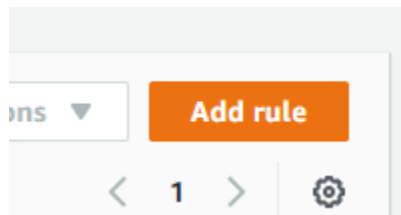
**Description**  
An AWS Config rule that is triggered by configuration changes to EC2 instances. Checks instance types.

**Last modified**  
12 seconds ago

**Function ARN**  
 `arn:aws:lambda:us-east-1:342103134475:function:ec2-config-change`

**Function URL** [Info](#)  
-

**Step 16:** Navigate back to Config dashboard and click on the “Add rule” button.



**Step 17:** Select rule type as “Create custom Lambda rule”. Click on the “Next” button.

## Specify rule type

Add rules to define the desired configuration setting of your AWS resources. Customize any of the following rules to suit your needs, or create a custom rule. To create a custom rule, you must create an AWS Lambda function for the rule.

### Select rule type

☐ Add AWS managed rule  
Customize any of the following rules to suit your needs.

☒ Create custom Lambda rule  
Create custom rules and add them to AWS Config. Associate each custom rule with an AWS Lambda function, which contains the logic that evaluates whether your AWS resources comply with the rule.

☐ Create custom rule using Guard  
Create custom rules using Guard Custom Policy that evaluates whether your AWS resources comply with the rule.

Cancel Next

**Step 18:** Set rule name as “ec2-change-rule”. Paste the copied lambda function ARN.

## Details

### Name

A unique name for the rule. 128 characters max. No special characters or spaces.

ec2-change-rule

### Description

*Describe what the rule evaluates and how to fix resources that don't comply.*

### AWS Lambda function ARN

The AWS Lambda function that evaluates whether your AWS resources comply with the rule when the rule is triggered.

arn:aws:lambda:us-east-1:342103134475:function:ec2-c

**Step 19:** Set the trigger type as "When configuration changes" and scope of change as Resources. Set Resource category as "All resource categories" and Select "AWS EC2 Instance", "AWS EC2 RouteTable", "AWS EC2 Subnet", "AWS EC2 VPC", "AWS EC2 NetworkInterface" as resources type.

## Trigger

### Trigger type

AWS Config evaluates resources when the trigger occurs.

☒ **When configuration changes**

Runs when there are changes to your specified AWS resources

☐ **Periodic**

Runs on the frequency that you choose

### Scope of changes

Choose when evaluations will occur.

☐ **All changes**

When any resource recorded by AWS Config is created, changed, or deleted

☒ **Resources**

When any resource that matches the specified type, or the type plus identifier, is created, changed, or deleted

☐ **Tags**

When any resource specified tag is changed, or deleted

## Resources

This rule can be triggered only when the recorded resources are created, edited, or deleted. Specify the resource editing the Settings page.

### Resource category

All resource categories ▼

### Resource type

Multiple Selected ▼

AWS EC2 Instance ✕

AWS EC2 RouteTable ✕

AWS EC2 Subnet ✕

AWS EC2 VPC ✕

AWS EC2 NetworkInterface ✕

AWS Config triggers the evaluation when any resource that matches the rule's scope changes in configuration. The evaluation runs after AWS Config sends a configuration item change notification.

**Step 20:** Click on the "Next" button.

Back

Next

Review the Config settings.

## Review and create

Review this rule before adding it to your account

### Details

Rule name

ec2-change-rule

Description

-

Config rule ARN

arn:aws:lambda:us-east-1:342103134475:function:ec2-config-change

### Trigger

Trigger type

- When configuration changes

Scope of changes

Resources

Resource types

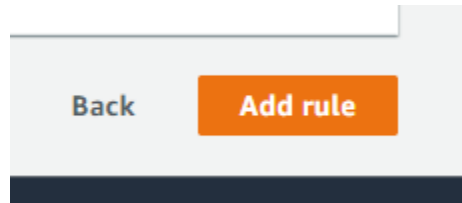
EC2 Instance,  
EC2 RouteTable,  
EC2 Subnet,  
EC2 VPC,  
EC2 NetworkInterface

Resource identifier

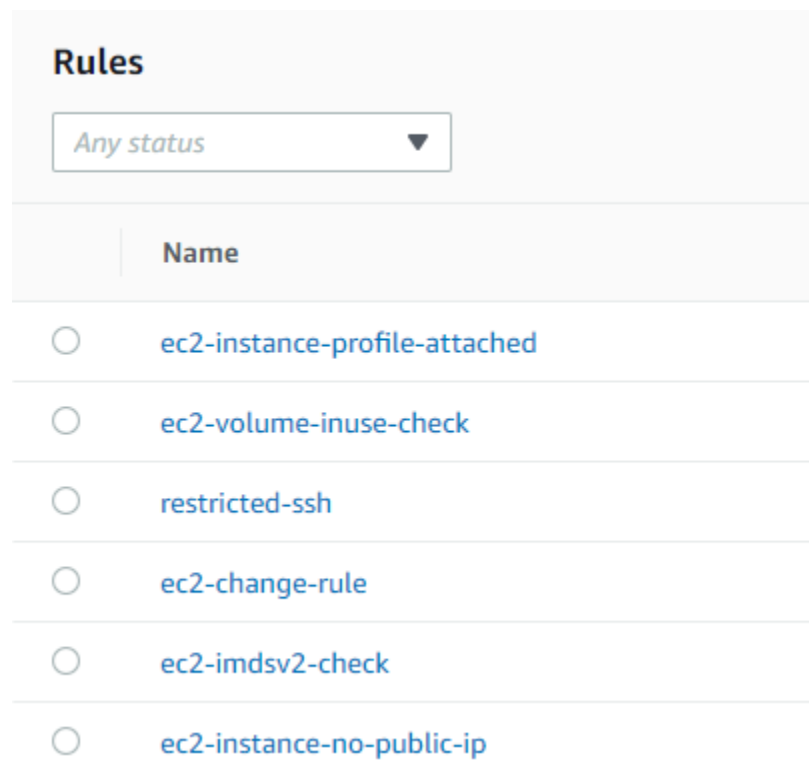
-

**Step 21:** Click on the “Add rule” button.

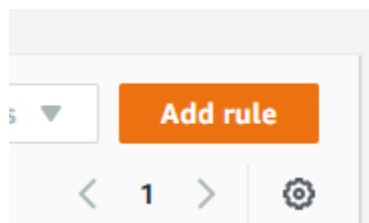




Successfully created the custom lambda Config rule.



**Step 22:** Again click on the “Add rule” button. Now add a custom rule using Guard.



**Step 23:** Set rule type as “Create custom rule using Guard” and click on “Next” button.

### Specify rule type

Add rules to define the desired configuration setting of your AWS resources. Customize any of the following rules to suit your needs, or create a custom rule. To create a custom rule, you must create an AWS Lambda function for the rule.

#### Select rule type

- ☐ Add AWS managed rule  
Customize any of the following rules to suit your needs.
- ☐ Create custom Lambda rule  
Create custom rules and add them to AWS Config. Associate each custom rule with an AWS Lambda function, which contains the logic that evaluates whether your AWS resources comply with the rule.
- ☒ Create custom rule using Guard  
Create custom rules using Guard Custom Policy that evaluates whether your AWS resources comply with the rule.

Cancel Next

**Step 24:** Set rule name as “check\_ec2\_eip\_compliance”. Set Guard runtime version as “guard-2.x.x”

Guard is a policy-as-code language that allows you to write policies that are enforced by AWS Config Custom Policy rules. Rules written using Guard can be created from the AWS Config console or by using the AWS Config rule APIs. AWS Config Custom Policy rules allow you to create AWS Config Custom rules without needing to use Java or Python to develop Lambda functions to manage your custom rules.

## Details

### Name

A unique name for the rule. 128 characters max. No special characters or spaces.

### Description

*Describe what the rule evaluates and how to fix resources that don't comply.*

### Guard runtime version

The Guard runtime utilized to execute the Custom Policy below.

☐ Enable debug logs

**Step 25:** Copy and paste the below code. This code will validate if any EC2 instances with an Elastic IP attached, are in a running state. If the EC2 instance is not in a running state, then the rule will mark the Amazon EC2 resource as non-compliant.

### Code:

```
let eipresource = relationships.*[ resourceType == 'AWS::EC2::EIP' ]

rule check_ec2_eip_compliance {
  when %eipresource !empty {
    configuration.state.name == "running"
  }
}
```

## Rule content

```
1
2 let eipresource = relationships.*[ resourceType == 'AWS::EC2::EIP' ]
3
4 rule check_ec2_eip_compliance {
5   when %eipresource != empty {
6     configuration.state.name == "running"
7   }
8 }
```

**Step 26:** Set scope of changes as “Resources” and select “AWS EC2 Instance” in the resource type.

## Trigger

### Trigger type

AWS Config evaluates resources when the trigger occurs.

☒ When configuration changes

Runs when there are changes to your specified AWS resources

☐ Periodic

Runs on the frequency that you

### Scope of changes

Choose when evaluations will occur.

☐ All changes

When any resource recorded by AWS Config is created, changed, or deleted

☒ Resources

When any resource that matches the specified type, or the type plus identifier, is created, changed, or deleted

☐ Tags

When specific change

## Resources

This rule can be triggered only when the recorded resources are created, edited, or deleted. Specify the resources when editing the Settings page.

Resource category

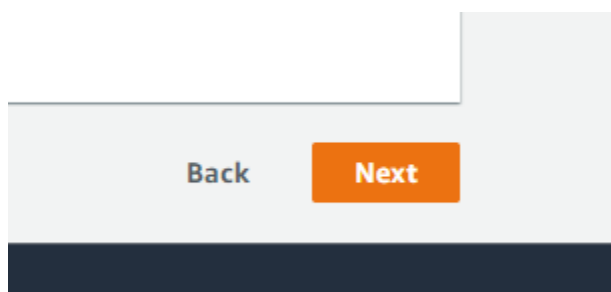
All resource categories ▼

Resource type

Multiple Selected ▼

AWS EC2 Instance X

**Step 27:** Click on the “Next” button.



Review the Config rule settings.

## Review and create

Review this rule before adding it to your account

Details	
Rule name	Guard runtime version
check_ec2_eip_compliance	Debug logs
Description	Disabled
-	

**Step 28:** Click on the “Add rule” button.

### Trigger

Trigger type

- When configuration changes

Resource types

EC2 Instance

Scope of changes
Resources

Resource identifier

-

### Tags

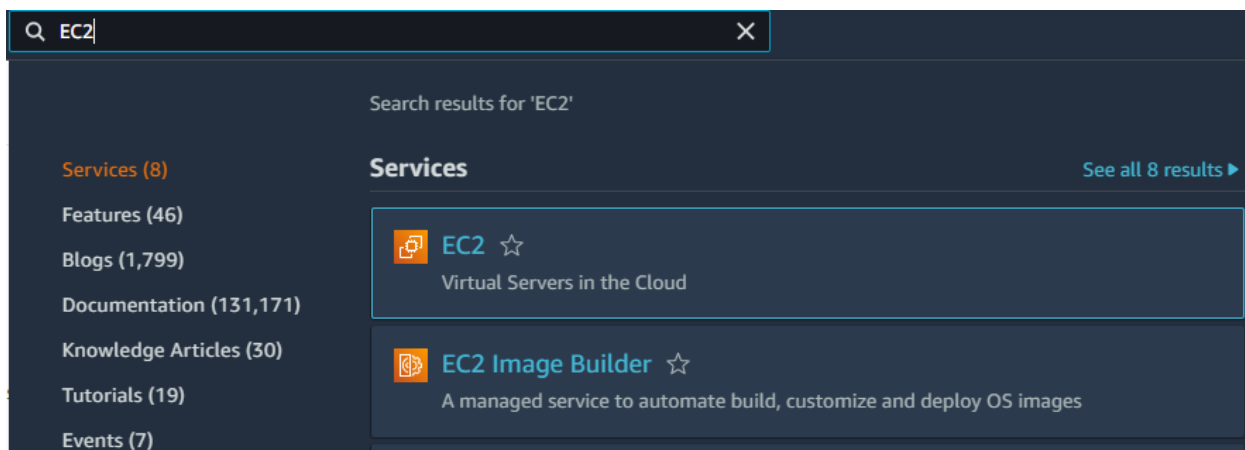
Key	Value

[Back](#)
[Add rule](#)

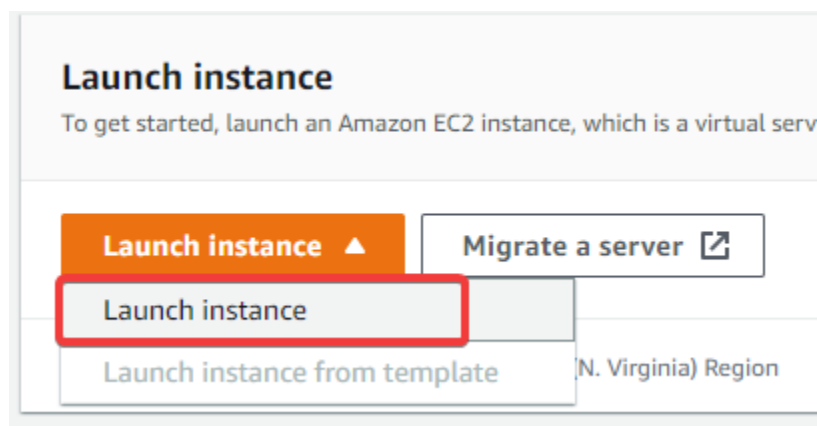
All the rules are created successfully. Now create resources and check out the working of AWS Config.

	Name	Remediation action	Type
<input type="radio"/>	ec2-instance-profile-attached	Not set	AWS managed
<input type="radio"/>	check_ec2_eip_compliance	Not set	Custom Policy
<input type="radio"/>	ec2-volume-inuse-check	Not set	AWS managed
<input type="radio"/>	restricted-ssh	Not set	AWS managed
<input type="radio"/>	ec2-change-rule	Not set	Custom Lambda
<input type="radio"/>	ec2-imdsv2-check	Not set	AWS managed
<input type="radio"/>	ec2-instance-no-public-ip	Not set	AWS managed

**Step 29:** Search for “EC2” in the search bar and navigate to EC2 Dashboard.



**Step 30:** Click on the “Launch Instance” button.



**Step 31:** Set Instance name as “lab-instance” and select “Amazon Linux” as AML.



Name

lab-instance

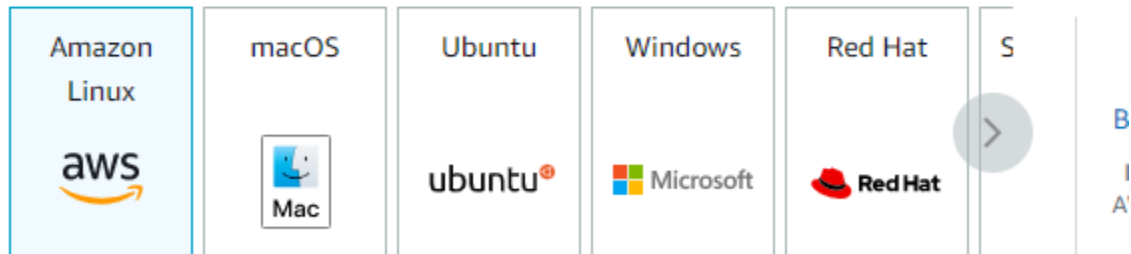
Ad

## ▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

 Search our full catalog including 1000s of application and OS images

### Quick Start



### Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type  
ami-05fa00d4c63e32376 (64-bit (x86)) / ami-05f3141013eebdc12 (64-bit (Arm))  
Virtualization: hvm    ENA enabled: true    Root device type: ebs

**Step 32:** Choose Instance type as “t2-micro” and proceed without a key pair.

## ▼ Instance type [Info](#)

### Instance type

t2.micro

Free tier eligible

Family: t2 1 vCPU 1 GiB Memory  
On-Demand Linux pricing: 0.0116 USD per Hour  
On-Demand Windows pricing: 0.0162 USD per Hour

## ▼ 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 to connect to the instance.

### Key pair name - *required*

Proceed without a key pair (Not recommended)

Default value ▼

**Step 33:** Select “Create security group” and set “Allow SSH traffic from anywhere”.

## Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow s instance.

☒ Create security group

☐ Select existing security group

We'll create a new security group called '**launch-wizard-1**' with the following rules:

☒ Allow SSH traffic from  
Helps you connect to your instance

Anywhere  
0.0.0.0/0 ▼

☐ Allow HTTPs traffic from the internet  
To set up an endpoint, for example when creating a web server

☐ Allow HTTP traffic from the internet  
To set up an endpoint, for example when creating a web server


**Step 34:** In the Advanced details , make Metadata accessibility “Enabled” and set “V2 only (token required)” for Metadata version.

Metadata accessible [Info](#)

Enabled

Metadata version [Info](#)

V2 only (token required)

 For V2 requests, you must include a session token in all instance metadata requests. Applications or agents that use V1 for instance metadata access will break.

**Step 35:** Click on the “Launch instance” button.

Cancel

Launch instance

Successfully created an instance.

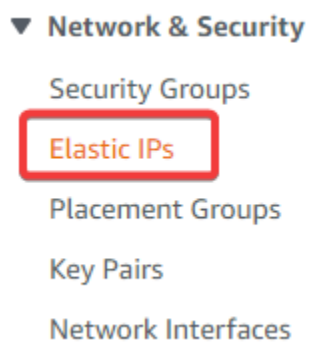


**Success**

Successfully initiated launch of instance (i-0621bb7af28e498c8)

► Launch log

**Step 36:** Click on “Elastic IPs” from the navigation pane.



**Step 37:** Click on the “Allocate Elastic IP address” button.



**Step 38:** Set public IPv4 address pool as “Amazon’s pool of IPv4 addresses”.

## Allocate Elastic IP address [Info](#)

### Elastic IP address settings [Info](#)

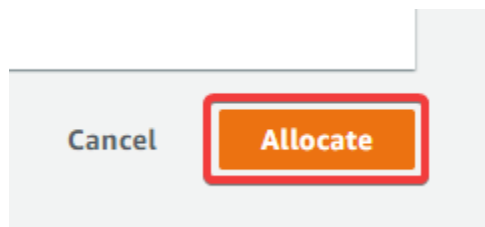
Network Border Group [Info](#)

us-east-1

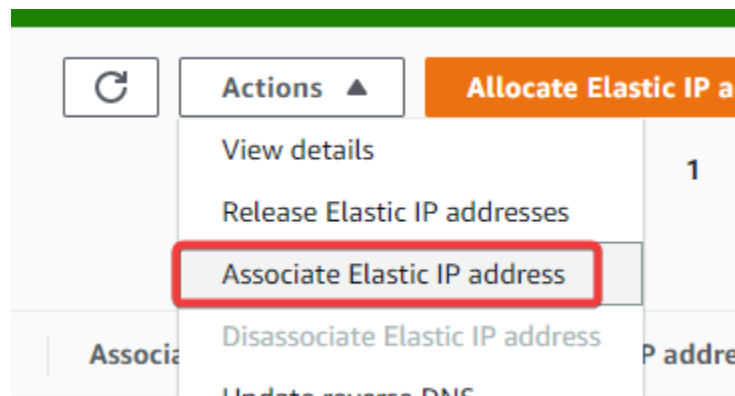
Public IPv4 address pool

- ☒ Amazon's pool of IPv4 addresses
- ☐ Public IPv4 address that you bring to your AWS account (option disabled pools found) [Learn more](#)
- ☐ Customer owned pool of IPv4 addresses (option disabled because no cus owned pools found) [Learn more](#)

**Step 39:** Click on the “Allocate” button.



**Step 40:** Select the allocated IP address and click on “Associate Elastic IP address” under the actions button.



**Step 41:** Choose the created instance id and allocated IP address.

**Elastic IP address: 3.84.107.59**

**Resource type**  
Choose the type of resource with which to associate the Elastic IP address.

☒ Instance  
☐ Network interface

**Warning:** If you associate an Elastic IP address to an instance that already has an Elastic IP address, the previously associated Elastic IP address will be disassociated but still allocated.

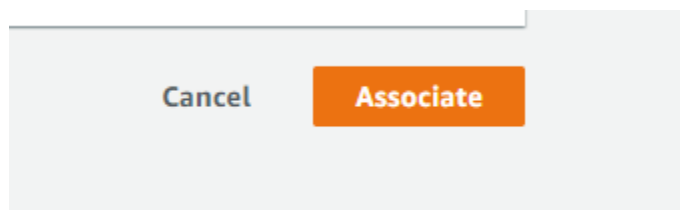
**Instance**  
Search: i-0621bb7af28e498c8

**Private IP address**  
The private IP address with which to associate the Elastic IP address.  
Search: 172.31.80.101

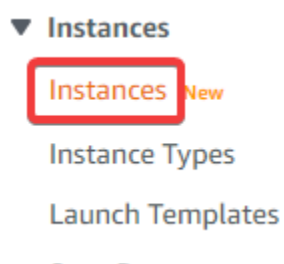
**Reassociation**  
Specify whether the Elastic IP address can be reassociated with a different resource if it already is associated with a resource.

☒ Allow this Elastic IP address to be reassociated

**Step 42:** Click on the “Associate” button.



**Step 43:** Click on “Instances” from the navigation pane.

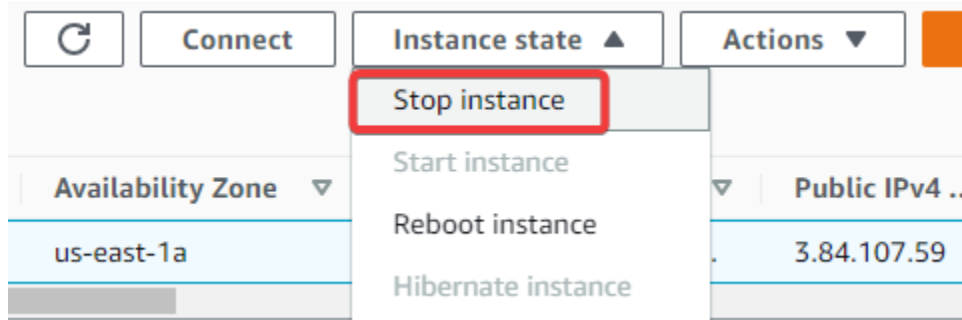


Elastic IP will be available for instance.

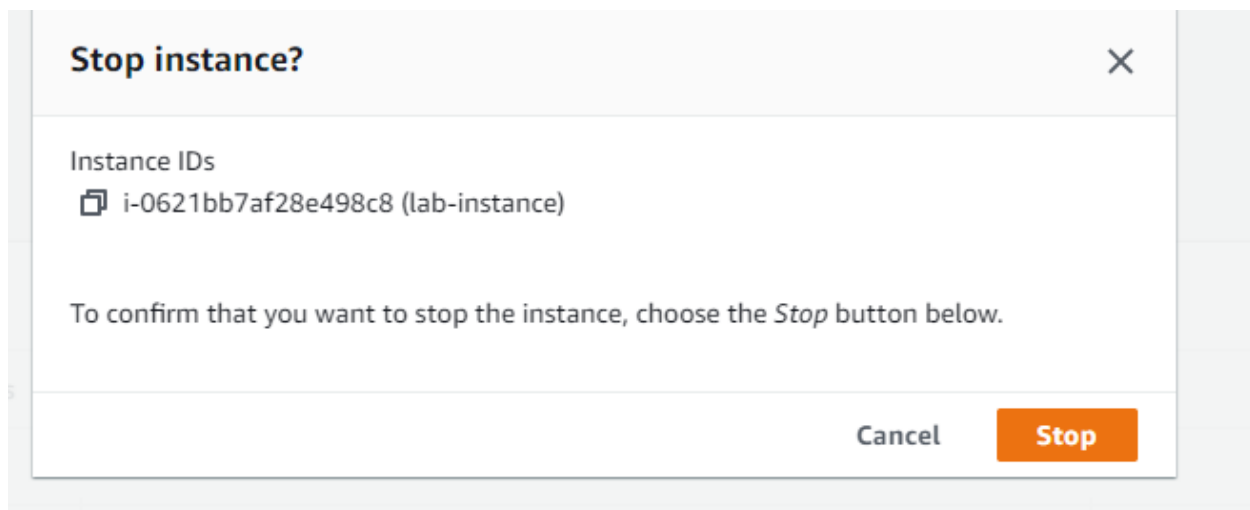
Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs
ec2-3-84-107-59.comp...	3.84.107.59	3.84.107.59	–

**Step 44:** Click on “Stop instance” under Instance state.





Click on the “Stop” button and confirm the action.



**Step 45:** Navigate back to AWS Config dashboard and check the created rules for compliance.

Rules				
<div> <div>View details</div> <div>Edit rule</div> <div>Actions ▾</div> <div>Add rule</div> </div>				
<div> <div>Any status ▾</div> <div>&lt; 1 &gt;</div> <div>⚙️</div> </div>				
	Name	Remediation action	Type	Compliance
<input type="radio"/>	<a href="#">ec2-instance-profile-attached</a>	Not set	AWS managed	⚠️ 1 Noncompliant resource(s)
<input type="radio"/>	<a href="#">check_ec2_eip_compliance</a>	Not set	Custom Policy	⚠️ 1 Noncompliant resource(s)
<input type="radio"/>	<a href="#">ec2-volume-inuse-check</a>	Not set	AWS managed	✅ Compliant
<input type="radio"/>	<a href="#">restricted-ssh</a>	Not set	AWS managed	⚠️ 1 Noncompliant resource(s)
<input type="radio"/>	<a href="#">ec2-change-rule</a>	Not set	Custom Lambda	⚠️ 1 Noncompliant resource(s)
<input type="radio"/>	<a href="#">ec2-imdsv2-check</a>	Not set	AWS managed	✅ Compliant
<input type="radio"/>	<a href="#">ec2-instance-no-public-ip</a>	Not set	AWS managed	⚠️ 1 Noncompliant resource(s)

**Step 46:** Click on “ec2-instance-profile-attached” .

Checks if an EC2 instance has an IAM profile attached to it. This rule is NON\_COMPLIANT if no IAM profile is attached to the EC2 instance.

## ec2-instance-profile-attached

▼ Rule details

Description

Checks if an Amazon Elastic Compute Cloud (Amazon EC2) instance has an Identity and Access Management (IAM) profile attached to it. This rule is NON\_COMPLIANT if no IAM profile is attached to the Amazon EC2 instance.

Config rule ARN

arn:aws:config:us-east-1:342103134475:config-rule/config-rule-f7fgde

Trigger type

- Oversized configuration changes
- Configuration changes

Scope of changes

Resources

Resource types

EC2 Instance

Last successful evaluation

✅ September 9, 2022 5:08 PM

Resource in scope is an EC2 Instance with ID “i-0621bb7af28e498c8”. This shows that this EC2 instance does not have an IAM profile attached to it.

Key	Type	Value	Description
IamInstanceProfileArnList	CSV	-	Comma-separated list of IAM profile Amazon Resource Name attached to Amazon EC2 instances.

▼ Resources in scope

View details

Noncompliant ▼

ID	Type	Status	Annotation
<input type="radio"/> i-0621bb7af28e498c8	EC2 Instance	-	-

**Step 47:** Click on “check\_ec2\_eip\_compliance”. This rule will validate if any EC2 instances with an Elastic IP attached, are in a running state. If the EC2 instance is not in a running state, then the rule will mark the Amazon EC2 resource as non-compliant.

## check\_ec2\_eip\_compliance

### ▼ Rule details

#### Description

#### Config rule ARN

arn:aws:config:us-east-1:342103134475:config-rule/config-rule-n4tndx

#### Trigger type

- Oversized configuration changes
- Configuration changes

#### Scope of changes

#### Resources

#### Resource types

EC2 Instance

#### Last successful evaluation

✓ September 9, 2022 5:16 PM

Resource in scope is an EC2 Instance with ID "i-0621bb7af28e498c8". EC2 instance with an Elastic IP attached is not in a running state.

### ▼ Resources in scope

Noncompliant ▼

	ID	Type	Status
<input type="radio"/>	i-0621bb7af28e498c8	EC2 Instance	-

**Step 48:** Click on "ec2-volume-inuse-check". Checks if EBS volumes are attached to EC2 instances. Optionally checks if EBS volumes are marked for deletion when an instance is terminated.

## ec2-volume-inuse-check

### ▼ Rule details

#### Description

Checks whether EBS volumes are attached to EC2 instances.

#### Config rule ARN

arn:aws:config:us-east-1:342103134475:config-rule/config-rule-geqxbb

#### Trigger type

- Oversized configuration changes
- Configuration changes

#### Scope of changes

#### Resources

#### Resource types

EC2 Volume

#### Last successful evaluation

✓ September 9, 2022 4:55 PM

### Parameters

**Step 49:** Click on “restricted-ssh” . Checks if the incoming SSH traffic for the security groups is accessible. The rule is COMPLIANT when IP addresses of the incoming SSH traffic in the security groups are restricted (CIDR other than 0.0.0.0/0). This rule applies only to IPv4.

## restricted-ssh

### ▼ Rule details

#### Description

Checks whether security groups that are in use disallow unrestricted incoming SSH traffic.

#### Config rule ARN

arn:aws:config:us-east-1:342103134475:config-rule/config-rule-s9he5m

#### Trigger type

- Oversized configuration changes
- Configuration changes

#### Scope of changes

#### Resources

#### Resource types

EC2 SecurityGroup

#### Last successful evaluation

✓ September 9, 2022 4:55 PM

Resource in scope is an EC2 Instance with ID “I-0621bb7af28e498c8”. This shows that SSH traffic in the security group is not restricted.

## ▼ Resources in scope

Noncompliant ▼

	ID	Type	Status
<input type="radio"/>	<a href="#">sg-0d0487b33378f909f</a>	EC2 SecurityGroup	-

**Step 50:** Click on “ec2-change-rule”. This rule will check if there are any changes performed in EC2 instance configuration. If the EC2 instance has any change in configurations, then the rule will mark the EC2 resource as non-compliant.

## ec2-change-rule

### ▼ Rule details

#### Description

##### Config rule ARN

arn:aws:config:us-east-1:342103134475:config-rule/config-rule-zhxskv

#### Trigger type

- Oversized configuration changes
- Configuration changes

#### Scope of changes

##### Resources

##### Resource types

- EC2 Instance
- EC2 RouteTable
- EC2 Subnet
- EC2 VPC
- EC2 NetworkInterface

#### Last successful evaluation

✓ September 9, 2022 5:08 PM

Resource in scope is an EC2 Instance with ID “i-0621bb7af28e498c8”. This shows that the instance running had some changes in configuration.

### ▼ Resources in scope

Noncompliant ▼

	ID	Type
<input type="radio"/>	i-0621bb7af28e498c8	EC2 Instance

**Step 51:** Click on “ec2-imdsv2-check”. This rule checks whether your Amazon Elastic Compute Cloud (Amazon EC2) instance metadata version is configured with Instance Metadata Service Version 2 (IMDSv2). The rule is NON\_COMPLIANT if the HttpTokens is set to optional.



## ec2-imdsv2-check

### ▼ Rule details

#### Description

Checks whether your Amazon Elastic Compute Cloud (Amazon EC2) instance metadata version is configured with Instance Metadata Service Version 2 (IMDSv2). The rule is NON\_COMPLIANT if the HttpTokens is set to optional.

#### Config rule ARN

arn:aws:config:us-east-1:342103134475:config-rule/config-rule-uj1fgs

#### Trigger type

- Oversized configuration changes
- Configuration changes

#### Scope of changes

Resources

#### Resource types

EC2 Instance

#### Last successful evaluation

✓ September 9, 2022 5:08 PM

This rule is compliant as we have enabled IMDSv2 for this instance.

**Step 52:** Click on “ec2-instance-no-public-ip”. This rule checks whether EC2 instances have a public IP association. The rule is NON\_COMPLIANT if the publicIp field is present in the Amazon EC2 instance configuration item. This rule applies only to IPv4.

## ec2-instance-no-public-ip

### ▼ Rule details

#### Description

Checks whether Amazon Elastic Compute Cloud (Amazon EC2) instances have a public IP association. The rule is NON\_COMPLIANT if the publicIp field is present in the Amazon EC2 instance configuration item. This rule applies only to IPv4.

#### Config rule ARN

arn:aws:config:us-east-1:342103134475:config-rule/config-rule-qry0k1

#### Trigger type

- Oversized configuration changes
- Configuration changes

#### Scope of changes

Resources

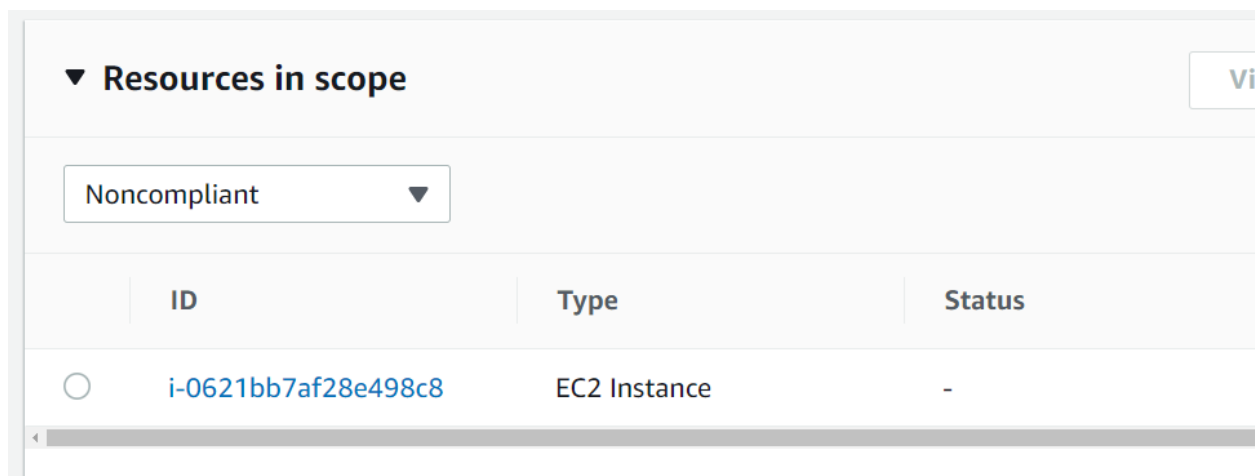
#### Resource types

EC2 Instance

#### Last successful evaluation

✓ September 9, 2022 5:08 PM

Resource in scope is an EC2 Instance with ID “I-0621bb7af28e498c8”. This shows that this instance does not have a public IP association.



The screenshot shows the 'Resources in scope' section of the AWS IAM console. A dropdown menu is set to 'Noncompliant'. Below it is a table with columns for ID, Type, and Status. One resource is listed: an EC2 Instance with ID i-0621bb7af28e498c8.

▼ Resources in scope				Vi
Noncompliant ▼				
	ID	Type	Status	
<input type="radio"/>	i-0621bb7af28e498c8	EC2 Instance	-	

**Step 53:** Click on “Dashboard” from the navigation pane.

**Dashboard**


Conformance packs

Rules

Resources

Resource inventory will provide the count of resources active in the AWS account.

## Resource inventory

View the inventory of your AWS and non-AWS resources. [Learn more](#) 

All resources ▼

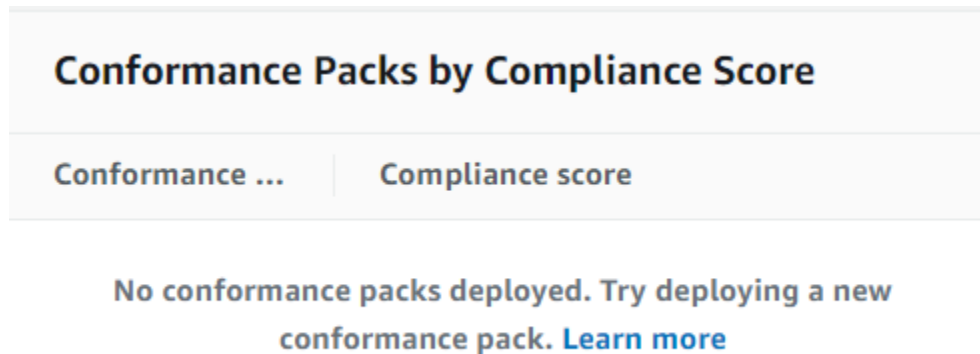
**Total resources**

**55**

Type	Count
CodeDeploy DeploymentConfig	17
IAM Role	10
EC2 Subnet	6
Config ResourceCompliance	4
IAM User	2
EC2 SecurityGroup	2
EC2 InternetGateway	1
EC2 Instance	1
Route53Resolver ResolverRule	1
EC2 VPC	1

There are no conformance packs deployed.

A conformance pack is a collection of AWS Config rules and remediation actions that can be easily deployed as a single entity in an account and a Region or across an organization in AWS Organizations.



**Step 54:** Click on “Conformance packs” from the navigation pane.

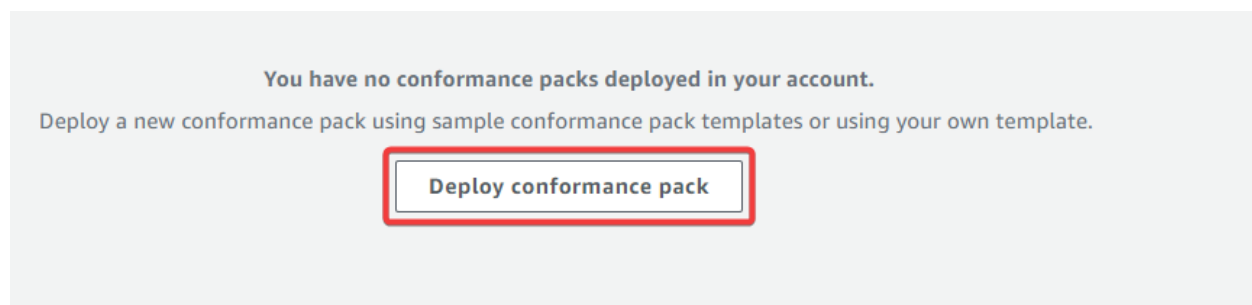
Dashboard

Conformance packs

Rules

Resources

**Step 55:** Click on the “Deploy conformance pack” button.



**Step 56:** Select “Use sample template” for conformance pack template and choose “Operational Best Practices for EC2”.

### Template details

**Conformance pack template**  
Every conformance pack is based on a template. A template is a YAML file that contains configuration information for regions where you want to deploy AWS Config rules and remediation actions.

☒ Use sample template

☐ Template is ready

### Sample template

**Select a sample template**  
This collection of sample templates will help you get started with conformance packs and quickly build your

Operational Best Practices for EC2 ▼

**Step 57:** Set conformance name as “ec2-conformance-pack”.

## Conformance pack details

Region

US East (N. Virginia)

Conformance pack name

Give the deployment of this template a name.

Conformance pack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-) but cannot include spaces.

**Step 58:** Click on the “Next” button.

Cancel

Previous

Next

Review the conformance pack configurations.

## Template details

Sample template

Operational Best Practices for EC2

## Conformance pack details

Region

US East (N. Virginia)

Conformance pack name

ec2-conformance-pack

**Step 59:** Click on the “Deploy conformance pack” button.

Cancel

Previous

Deploy conformance pack

**Step 60:** Click on “ec2-conformance-pack”.



ec2-conformance-pack

Deployment status

✓ Completed

INSUFFICIENT DATA

Compliance score

View

It will list all the rules available inside the conformance pack.

## Rules (20)

 *Filter rules by name or compliance status*

### Name

[ec2-instance-detailed-monitoring-enabled-conformance-pack-ylgvrjita](#)

[ec2-resources-protected-by-backup-plan-conformance-pack-ylgvrjita](#)

[ec2-managedinstance-association-compliance-status-check-conformance-pack-ylgvrjita](#)

[ec2-stopped-instance-conformance-pack-ylgvrjita](#)

[ec2-imdsv2-check-conformance-pack-ylgvrjita](#)

[cloudwatch-alarm-resource-check-conformance-pack-ylgvrjita](#)

[ec2-instance-managed-by-systems-manager-conformance-pack-ylgvrjita](#)

[ec2-instance-profile-attached-conformance-pack-ylgvrjita](#)

[eip-attached-conformance-pack-ylgvrjita](#)

[ec2-no-amazon-key-pair-conformance-pack-ylgvrjita](#)

**Step 61:** Click on “Rules” from the navigation pane.

Dashboard

Conformance packs

**Rules**

Resources

▼ Aggregators

Check out the compliance for all the created rules.

<input checked="" type="radio"/>	ec2-stopped-instance-confor...	Not set	AWS managed	✔ Compliant
<input checked="" type="radio"/>	ec2-instance-multiple-eni-ch...	Not set	AWS managed	✔ Compliant
<input type="radio"/>	ec2-change-rule	Not set	Custom Lambda	⚠ 1 Noncompliant resource(s)
<input checked="" type="radio"/>	ec2-resources-protected-by-...	Not set	AWS managed	-
<input checked="" type="radio"/>	ec2-token-hop-limit-check-c...	Not set	AWS managed	✔ Compliant
<input checked="" type="radio"/>	ec2-instance-managed-by-sy...	Not set	AWS managed	⚠ 1 Noncompliant resource(s)
<input checked="" type="radio"/>	cloudwatch-alarm-resource-c...	Not set	AWS managed	⚠ 1 Noncompliant resource(s)
<input checked="" type="radio"/>	ec2-no-amazon-key-pair-con...	Not set	AWS managed	-
<input checked="" type="radio"/>	ec2-instance-detailed-monit...	Not set	AWS managed	⚠ 1 Noncompliant resource(s)
<input type="radio"/>	restricted-ssh	Not set	AWS managed	⚠ 1 Noncompliant resource(s)
<input type="radio"/>	ec2-imdsv2-check	Not set	AWS managed	✔ Compliant

Successfully created AWS Config rules and checked if the created resources are compliant or non compliant.

## References:

1. AWS Config  
(<https://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html>)