

AWS Config - Demo



Simple setup

AWS Config automatically discovers your AWS resources and starts recording configuration changes. You can create Config rules from a set of pre-built managed rules to get started.



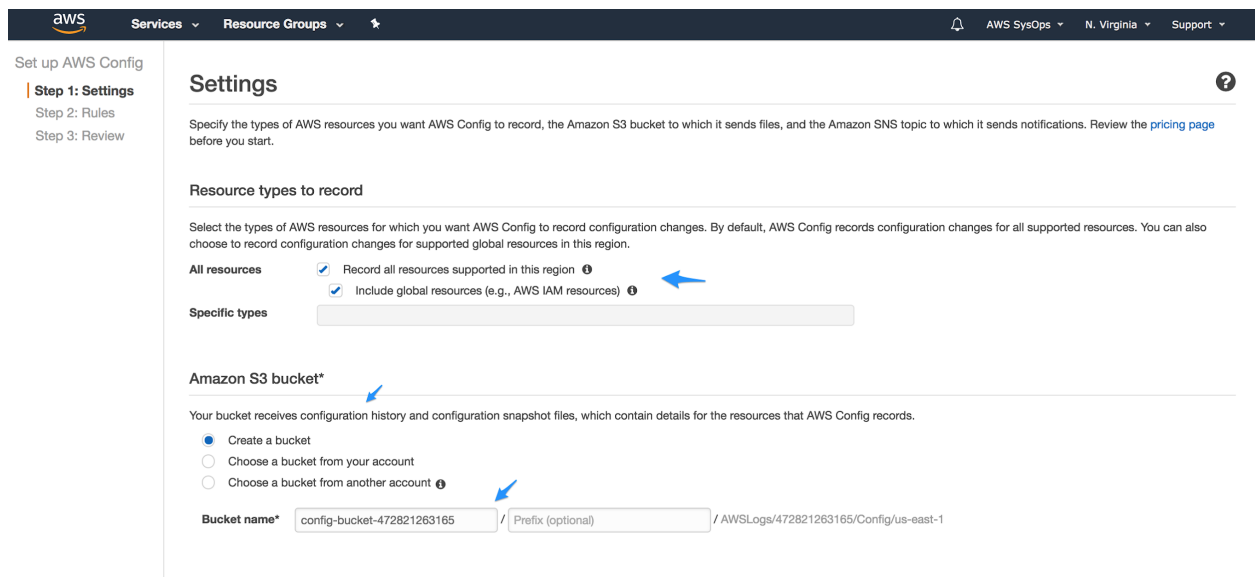
Customize rules

You can configure any of the pre-built rules to suit your needs, or create your own rules using AWS Lambda to check configurations for compliance.



Continuous compliance

AWS Config continuously records configuration changes to resources and automatically evaluates these changes against relevant rules. You can use a dashboard to assess overall configuration compliance.



Step 1: Settings

Step 2: Rules

Step 3: Review

Amazon SNS topic

- ☒ Stream configuration changes and notifications to an Amazon SNS topic.  [Learn more.](#)

- ☒ Create a topic
- ☐ Choose a topic from your account
- ☐ Choose a topic from another account 

Topic name* config-topic 

AWS Config role*

Grant AWS Config read-only access to your AWS resources so that it can record configuration information, and grant it permission to send this information to Amazon S3 and Amazon SNS.

- ☒ Create AWS Config service-linked role
- ☐ Choose a role from your account

* Required

Cancel

Next 

Step 1: Settings

Step 2: Rules

Step 3: Review

AWS Config rules 

AWS Config can check the configuration of your resources against rules that you define. Choose one or more of the following rules to get started. After setting up AWS Config, you can customize these rules, set up other rules provided by AWS Config, or create your own rules.

Learn more about [AWS Config rules and pricing details](#).

elp

<< < Viewing 1 - 1 of 1 AWS managed rules > >>

elp-attached

Checks whether all EIP addresses allocated to a VPC are attached to EC2 instances or in-use ENIs.

EC2

You can customize these rules and add other rules after completing the setup process.

Cancel

Previous

Skip

Next 

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.

AWS Config rules (1)

eip-attached Checks whether all EIP addresses allocated to a VPC are attached to EC2 instances or in-use ENIs.

Settings

Resource types All resources (including global resources)

Amazon S3 bucket config-bucket-472821263165

Amazon SNS topic config-topic

AWS Config role AWSServiceRoleForConfig

Cancel Previous **Confirm**

Config Dashboard

Status

Resources

Total resource count	69
Resource types	Total
EC2 SecurityGroup	53
EC2 Subnet	6
CloudWatch Alarm	3
EC2 InternetGateway	1
EC2 VPC	1
RDS DBSubnetGroup	1
CloudTrail Trail	1
RDS DBSecurityGroup	1
EC2 RouteTable	1
EC2 NetworkAcl	1

[View all 69 resources](#)

Config rule compliance

Resource compliance

Evaluate your AWS resource configuration using Config rules

Add rules to define the desired configuration settings for your AWS resources.

Noncompliant rule(s)

Add rule

Noncompliant resource(s)

Noncompliant rules

Rule name	Compliance
All rules compliant	

Rules

Status

Rules represent your desired configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and summarizes the results in the following table.

Add rule

Estimate rules cost

Refresh

Compliance status **Filter**

Rule name	Compliance	Edit rule
eip-attached	No resources in scope	Edit

AWS Config

- Dashboard
- Rules
- Resources
- Settings**
- Authorizations

Aggregated view

- Rules
- Aggregators

What's new

Learn More

- [Documentation](#)
- [Partners](#)
- [FAQs](#)
- [Pricing](#)
- [Cost estimator](#)

Settings

Status ?

Recording is on 

Resource types to record

Select the types of AWS resources for which you want AWS Config to record configuration changes. By default, AWS Config records configuration changes for all supported resources. You can also choose to record configuration changes for supported global resources in this region.

All resources ☒ Record all resources supported in this region ⓘ

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

Specific types

Data retention period Default period is 7 years 

☐ Set a custom retention period for configuration items recorded by AWS Config.

Now let's launch an EC2 Instance in us-east-1 region and then attach an Elastic IP to that Instance.

```
INBL2-42RG3QD:~ mahtab.alam$ aws ec2 run-instances --image-id ami-013be31976ca2c322 --count 1 --instance-type t2.micro
--key-name sysops --profile mahtab-sysops
{
  "Instances": [
    {
      "Monitoring": {
        "State": "disabled"
      },
      "PublicDnsName": "",
      "StateReason": {
        "Message": "pending",
        "Code": "pending"
      },
      "State": {
        "Code": 0,
        "Name": "pending"
      },
      "EbsOptimized": false,
      "LaunchTime": "2018-11-11T15:33:42.000Z",
      "PrivateIpAddress": "172.31.92.218",
      "ProductCodes": [],
      "VpcId": "vpc-2a011251",
      "CpuOptions": {
        "CoreCount": 1,
        "ThreadsPerCore": 1
      },
      "StateTransitionReason": "",
      "InstanceId": "i-0f75322c7eab4f14b",
      "ImageId": "ami-013be31976ca2c322",
      "PrivateDnsName": "ip-172-31-92-218.ec2.internal",
      "KeyName": "sysops",
      "SecurityGroups": [
        {
          "GroupName": "default",
          "GroupId": "sg-9446a7df"
        }
      ],
      "ClientToken": "",
      "SubnetId": "subnet-d070a0fe",
      "InstanceType": "t2.micro",
    }
  ]
}
```

 **Note that when we don't specify the security groups while launching Instance, the Instance will get assigned the default security group of the VPC**

Next lets allocate an Elastic IP

```
[INBL2-42RG3QD:~ mahtab.alam$ aws ec2 allocate-address --domain vpc --profile mahtab-sysops
{
  "PublicIp": "100.24.226.206",
  "Domain": "vpc",
  "AllocationId": "eipalloc-098bf8245213d5972",
  "PublicIpv4Pool": "amazon"
}
INBL2-42RG3QD:~ mahtab.alam$
```

Lets attach this EIP with the EC2 Instance

[Addresses](#) > Associate address

Associate address

Select the instance OR network interface to which you want to associate this Elastic IP address (100.24.226.206)

Resource type ☒ Instance ☐ Network interface

Instance

Private IP

Reassociation ☐ Allow Elastic IP to be reassociated if already attached

Warning
If you associate an Elastic IP address with your instance, your current public IP address is released. [Learn more](#).

[Cancel](#) [Associate](#)

```
[INBL2-42RG3QD:~ mahtab.alam$ aws ec2 describe-addresses --profile mahtab-sysops
{
  "Addresses": [
    {
      "Domain": "vpc",
      "PublicIpv4Pool": "amazon",
      "InstanceId": "i-0f75322c7eab4f14b",
      "NetworkInterfaceId": "eni-0400e391c87abff3a",
      "AssociationId": "eipassoc-03c2cb73f1910503c",
      "NetworkInterfaceOwnerId": "472821263165",
      "PublicIp": "100.24.226.206",
      "AllocationId": "eipalloc-098bf8245213d5972",
      "PrivateIpAddress": "172.31.92.218"
    }
  ]
}
INBL2-42RG3QD:~ mahtab.alam$
```

At this point the Elastic IP is attached to the Instance, so our eip-attached config rule will show it as compliant

eip-attached

Description Checks whether all EIP addresses allocated to a VPC are attached to EC2 instances or in-use ENIs.

Trigger type Configuration changes

Scope of changes Resources

Resource types EC2 EIP

Config rule ARN arn:aws:config:us-east-1:472821263165:config-rule/config-rule-kpcju4

Parameters null

Overall rule status Not available

Re-evaluate Delete results Edit

Lets manually re-evaluate the eip-attached rule

Resources evaluated

Resource actions

Resource identifier	Resource type	Compliance	Last successful invocation	Last successful evaluation
---------------------	---------------	------------	----------------------------	----------------------------

Rules

Status ?

Rules represent your desired configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and summarizes the results in the following table.

Add rule

Estimate rules cost

Compliance status

Filter

Rule name	Compliance	Edit rule
eip-attached	Compliant	

eip-attached

Re-evaluate Delete results Edit

Description Checks whether all EIP addresses allocated to a VPC are attached to EC2 instances or in-use ENIs.

Trigger type Configuration changes

Scope of changes Resources

Resource types EC2 EIP

Config rule ARN arn:aws:config:us-east-1:472821263165:config-rule/config-rule-kpcju4

Parameters null

Overall rule status Last successful invocation on November 11, 2018 at 9:18:00 PM
Last successful evaluation on November 11, 2018 at 9:18:00 PM

Resources evaluated

Resource actions

Resource identifier	Resource type	Compliance	Last successful invocation	Last successful evaluation
eipalloc-098bf8245213d5972	EC2 EIP	Compliant	November 11, 2018 9:18:00 PM	November 11, 2018 9:18:00 PM

Dashboard

Rules
Resources
Settings
Authorizations

Aggregated view

Rules
Aggregators

What's new

Learn More

[Documentation](#)[Partners](#)[FAQs](#)[Pricing](#)[Cost estimator](#)

Config Dashboard

Status ?

Resources

Total resource count 160

Top 10 resource types Total

EC2 SecurityGroup 53

IAM Role 46

S3 Bucket 20

IAM Policy 16

EC2 Subnet 6

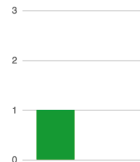
IAM User 5

CloudWatch Alarm 3

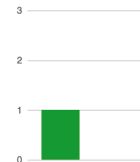
EC2 InternetGateway 1

EC2 Instance 1

Config rule compliance

0
Noncompliant
rule(s)

Resource compliance

0
Noncompliant
resource(s)

Noncompliant rules

Rule name	Compliance
All rules compliant	

Now lets disassociate the EIP from EC2 Instance

Allocate new address Actions

Filter by tags and attributes or search by keyword

Name	Name	Elastic IP	Allocation ID	Instance	Private IP address	Scope	Association ID	Netw
		100.24.226.206	eipalloc-098bf8245...	i-0f75322c7eab4f14b	172.31.92.218	vpc	eipassoc-03c2cb73f...	eni-0...

Disassociate address

Are you sure you want to disassociate this Elastic IP address?

Elastic IP 100.24.226.206

Instance ID i-0f75322c7eab4f14b

Network Interface ID eni-0400e391c87abff3a

Cancel Disassociate address

Address: 100.24.226.206

Description	Tags
Elastic IP	100.24.226.206
Address Pool	amazon
Private IP address	172.31.92.218
Association ID	eipassoc-03c2cb73f1910503c

Allocation ID	Instance	Scope	Public DNS
eipalloc-098bf8245213d5972	i-0f75322c7eab4f14b	vpc	ec2-100-24-226-206.compute-1.amazonaws.com

```
INBL2-42RG3QD:~ mahtab.alam$ aws ec2 describe-addresses --profile mahtab-sysops
{
  "Addresses": [
    {
      "PublicIp": "100.24.226.206",
      "Domain": "vpc",
      "AllocationId": "eipalloc-098bf8245213d5972",
      "PublicIpv4Pool": "amazon"
    }
  ]
}
INBL2-42RG3QD:~ mahtab.alam$
```

Now our eip-attached rule will show non-compliant for the EIP

Amazon S3 > config-bucket-472821263165 / AWSLogs / 472821263165 / Config

Overview

Q Type a prefix and press Enter to search. Press ESC to clear.

Upload Create folder Actions

US East (N. Virginia)

Name	Last modified	Size	Storage class
ConfigWritabilityCheckFile	Nov 11, 2018 8:53:05 PM GMT+0530	0 B	Standard

Viewing 1 to 1

Search mail

1-50 of 18,840

Primary Social Promotions

Primary	Subject	Time
AWS Notifications 5	[AWS Config:us-east-1] Config Rules Evaluation Started for Account 472821263165 - { "awsAccountId": "472821263165", ...	9:37 PM
AWS Notifications	[AWS Config:us-east-1] AWS::Config::ResourceCompliance AWS::EC2::EIP/eipalloc-098bf8245213d5972 C... - View the T...	9:19 PM
AWS Notifications	[AWS Config:us-east-1] AWS::EC2::EIP eipalloc-098bf8245213d5972 is COMPLIANT with eip-attached in... - View the Ti...	9:18 PM
AWS Notifications	[AWS Config:us-east-1] AWS::EC2::Instance i-0f75322c7eab4f14b Updated in Account 472821263165 - View the Timelin...	9:18 PM
AWS Notifications	[AWS Config:us-east-1] AWS::EC2::NetworkInterface eni-0400e391c87abff3a Updated in Account 472821... - View the Ti...	9:18 PM
AWS Notifications	[AWS Config:us-east-1] AWS::EC2::EIP 100.24.226.206 Created in Account 472821263165 - View the Timeline for this Re...	9:18 PM
AWS Notifications	[AWS Config:us-east-1] AWS::EC2::Volume vol-0e6da5a4e5e969c47 Created in Account 472821263165 - View the Timeli...	9:12 PM
AWS Notifications	[AWS Config:us-east-1] AWS::EC2::NetworkInterface eni-0400e391c87abff3a Created in Account 472821... - View the Ti...	9:12 PM
AWS Notifications	[AWS Config:us-east-1] AWS::EC2::Instance i-0f75322c7eab4f14b Created in Account 472821263165 - View the Timelin...	9:12 PM

AWS Config

Dashboard

Rules

Resources

Settings

Authorizations

Aggregated view

Rules

Aggregators

What's new

Learn More

[Documentation](#)

[Partners](#)

[FAQs](#)

[Pricing](#)

Cost estimator

Edit -eip-attached

AWS Config evaluates your AWS resources against this rule when it is triggered.

Name* eip-attached

Description Checks whether all EIP addresses allocated to a VPC are attached to EC2 instances or in-use ENIs.

Managed rule name EIP_ATTACHED

Trigger

AWS Config evaluates resources when the trigger occurs.

Trigger type* ☒ Configuration changes ☐ Periodic

Scope of changes* ☒ Resources ☐ Tags ☐ All changes

Resources* EC2: EIP

Resource identifier (optional)

Note that we could have set the Trigger type to Periodic

AWS Config > resources > i-0f75322c7eab4f14b > configuration

EC2 Instance i-0f75322c7eab4f14b

on November 11, 2018 9:17:59 PM IST (UTC+05:30)

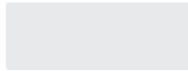
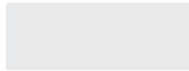
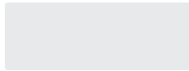
Managed instance information

Manage resource

Configuration timeline

Compliance timeline

Note that from config dashboard's resources section we can see the timeline for any resource that is under recording of Config and all the changes happened to that resource



Now



5 Changes

Configuration Details

View Details

Amazon Resource Name arn:aws:ec2:us-east-1:472821263165:instance/i-0f75322c7eab4f14b

Resource type AWS::EC2::Instance

Resource ID i-0f75322c7eab4f14b

Resource name null

Instance Type t2.micro

Instance state running

Private DNS ip-172-31-92-218.ec2.internal

Private Ips 172.31.92.218

Public DNS ec2-100-24-226-206.compute-1.amazonaws.com

AWS Config

Dashboard

Rules

Resources

Settings

Authorizations

Aggregated view

Rules

Aggregators

What's new

Learn More

[Documentation](#)

[Partners](#)

[FAQs](#)

[Pricing](#)

Cost estimator

Settings

Status

Recording is

Turn off

Resource type

Select the types of resources. You can select all resources or specific types.

All resources

Specific types

Data retention period

Default period is 7 years

Set a custom retention period for configuration items recorded by AWS Config.

Stop recording

Stop recording? AWS Config will no longer record changes to your resource configurations. Evaluations that are triggered by configuration changes will not occur. Configurations that are already recorded will still be accessible. You can resume recording any time.

Cancel

Continue