AWS Config - Demo

Simple setup

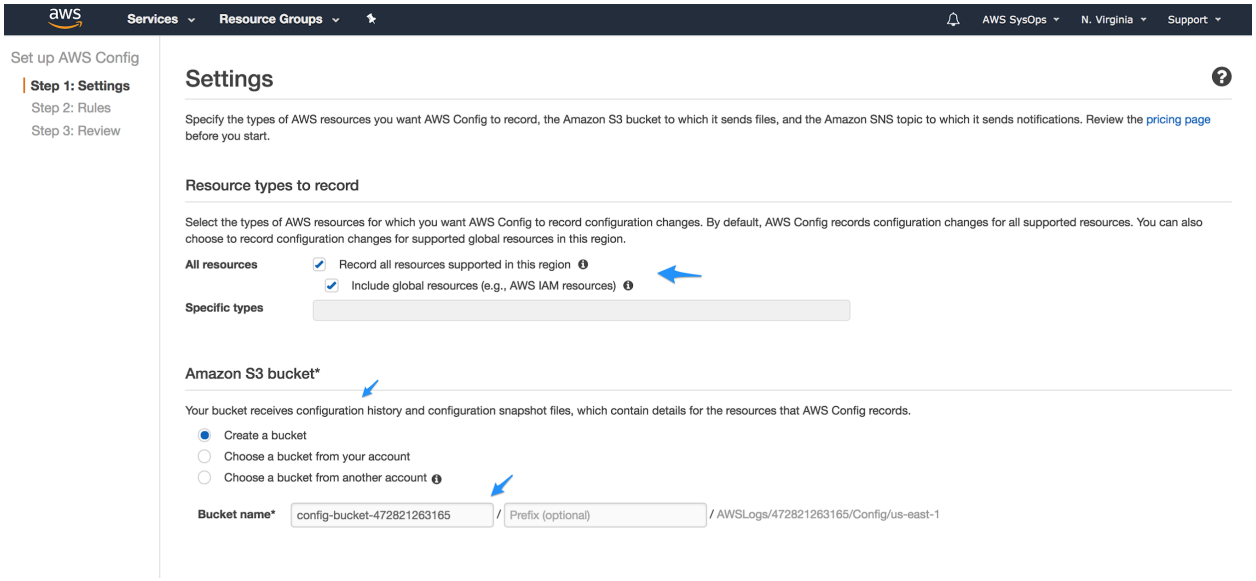
AWS Config automatically discovers your AWS resources and starts recording configuration changes. You can create Config rules from a set of pre-built managed rules to get started.

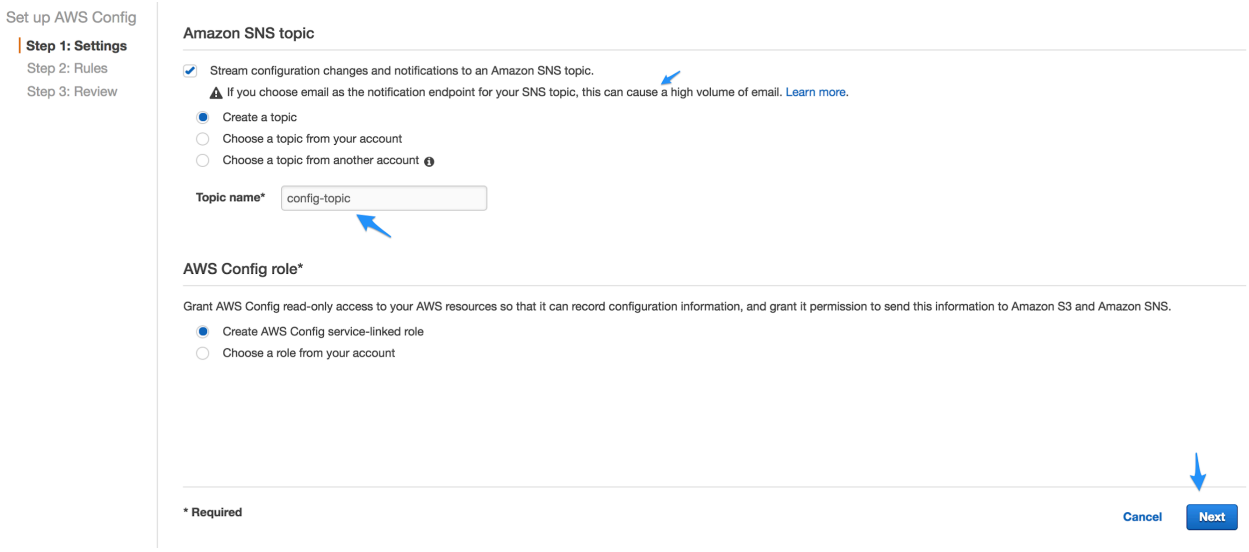
Customize rules

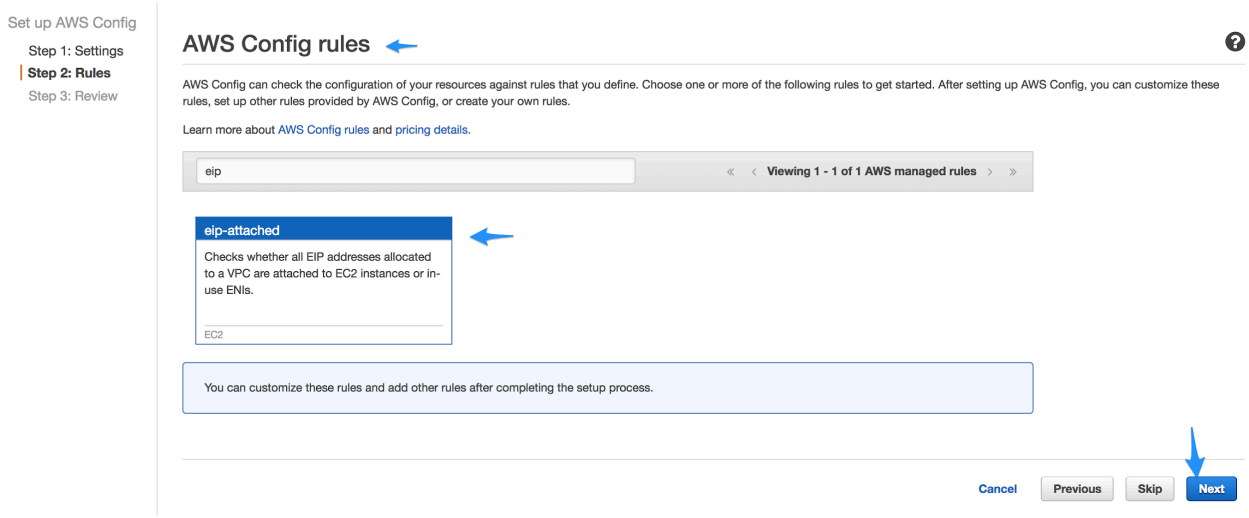
You can configure any of the pre-built rules to suit your needs, or create your own rules using AWS Lambda to check configurations for compliance.

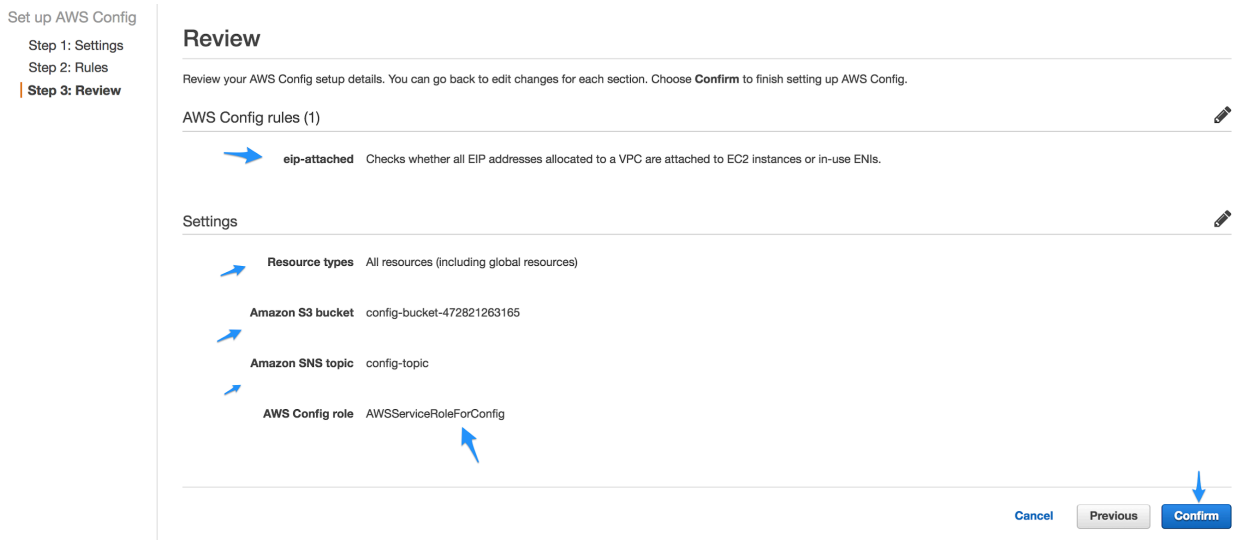
Continuous compliance

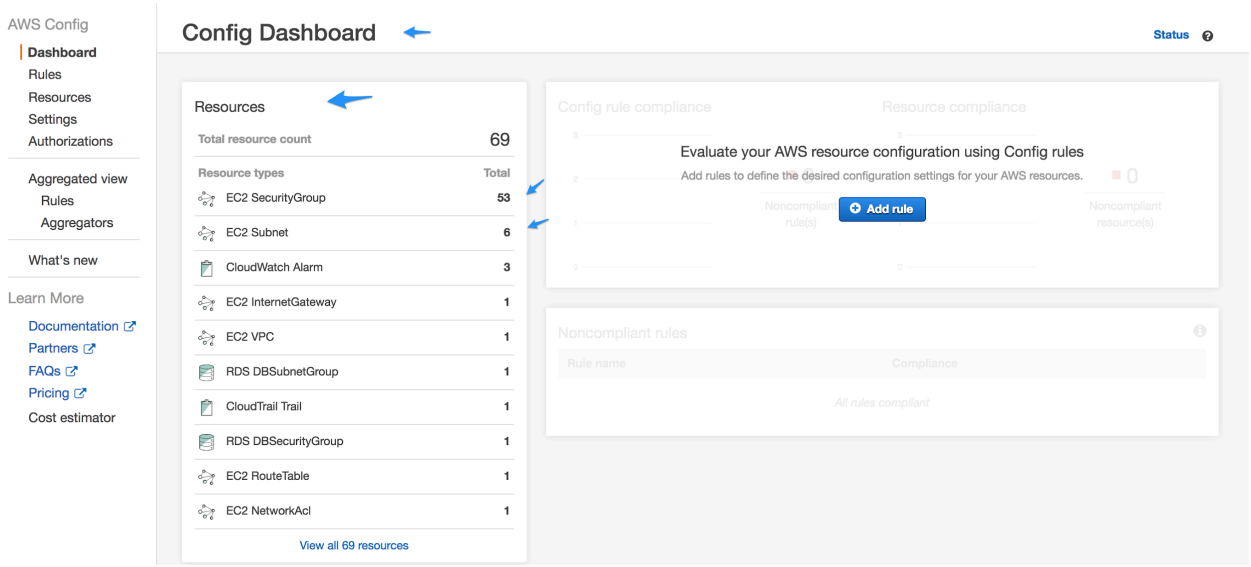
AWS Config continuously records configuration changes to resources and automatically evaluates these changes against relevant rules. You can use a dashboard to assess overall configuration compliance.

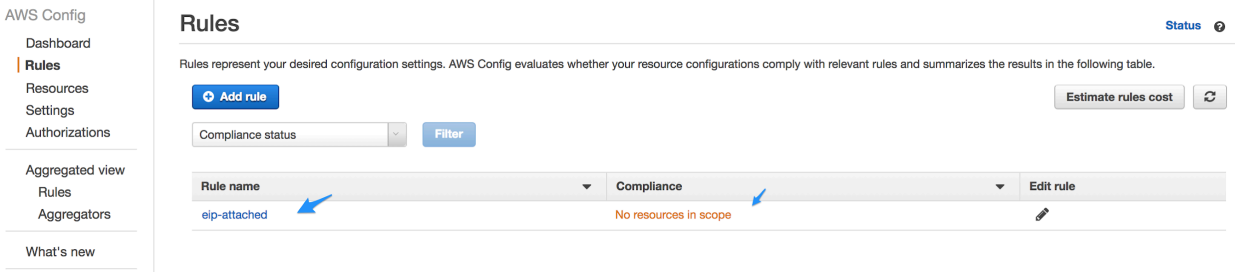


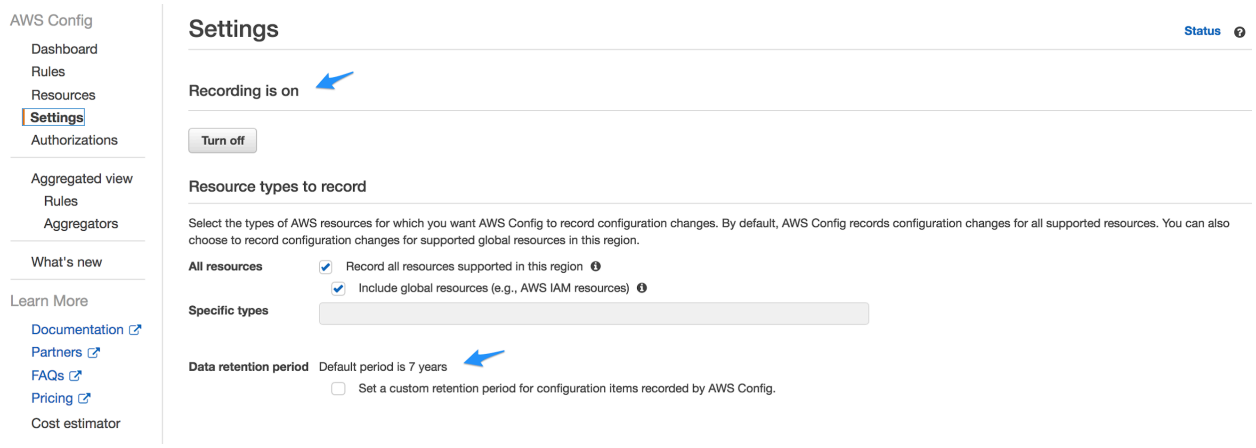

Set up AWS Config
Step 1: Settings
Step 2: Rules
Step 3: Review
Amazon SNS topic
Stream configuration changes and notifications to an Amazon SNS topic.
If you choose email as the notification endpoint for your SNS topic, this can cause a high volume of email. Learn more.
Create a topic
Choose a topic 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


Set up AWS Config
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.
eip
Viewing 1 - 1 of 1 AWS managed rules
eip-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


Set up AWS Config
Step 1: Settings
Step 2: Rules
Step 3: Review
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


AWS Config
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 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.
Add rule
Noncompliant rule(s)
Noncompliant resource(s)
Noncompliant rules
Rule name
Compliance
All rules compliant


AWS Config
Dashboard
Rules
Resources
Settings
Authorizations
Aggregated view
Rules
Aggregators
What's new
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
No resources in scope



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

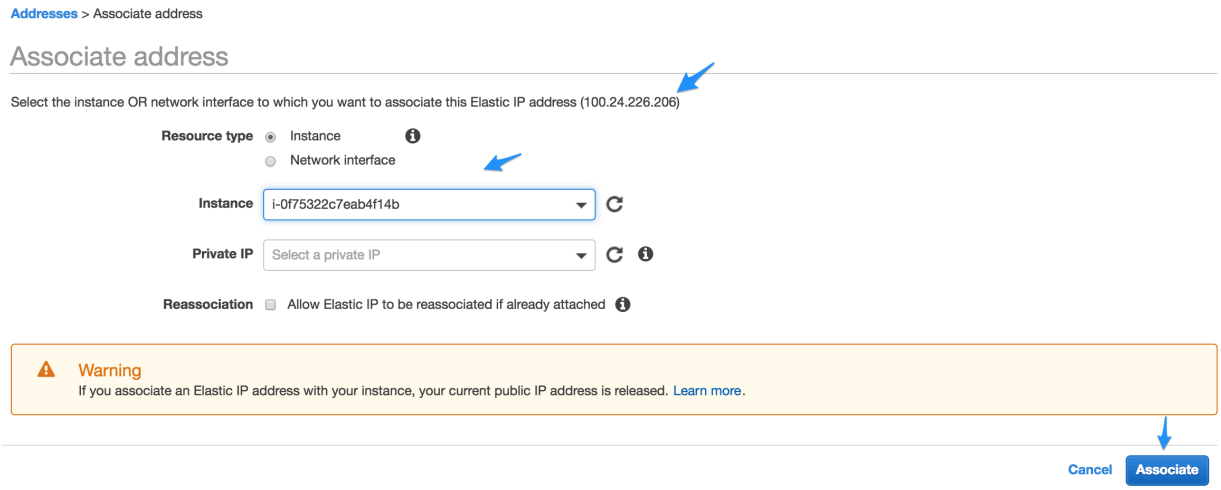
```
INBL2-42RG3QD:~ mahtab.alam$ aws ec2 run-instances --image-id ami-013be31976ca2c322 --count 1 --instance-type t2.micro
--key-name sysops --profile mahtab-sysops
{
    "Instances": [
        {
            "Monitoring": {
                "State": "disabled"
            },
            "PublicDnsName": "",
            "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

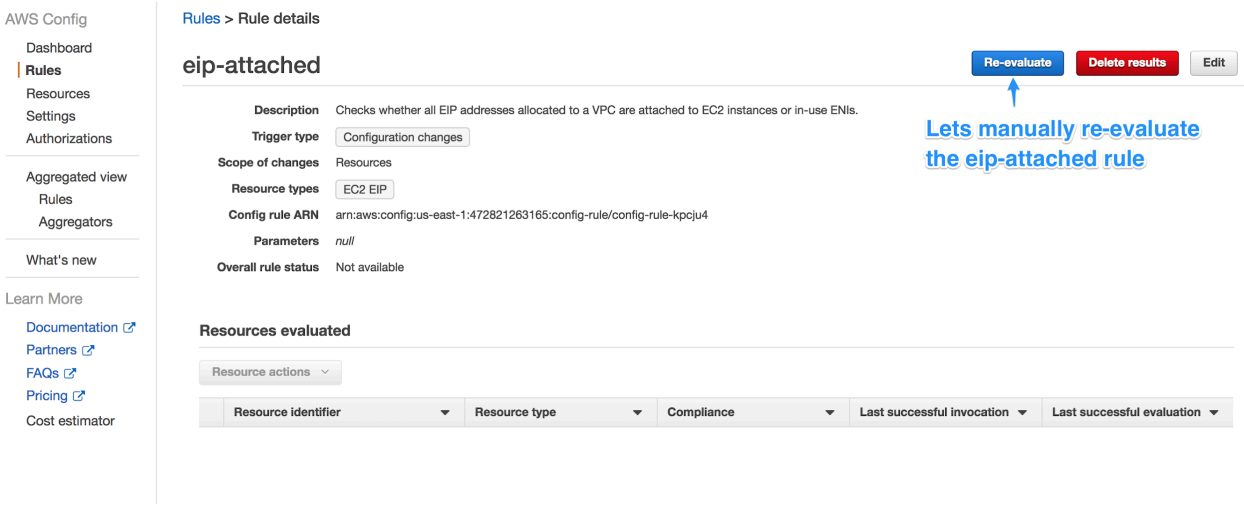
```
INBL2-42RG3QD:~ mahtab.alam$ aws ec2 allocate-address --domain vpc --profile mahtab-sysops
{
    "PublicIp": "100.24.226.206",
    "Domain": "vpc",
    "AllocationId": "eipalloc-098bf8245213d5972",
    "PublicIpv4Pool": "amazon"
}
INBL2-42RG3QD:~ mahtab.alam$
```

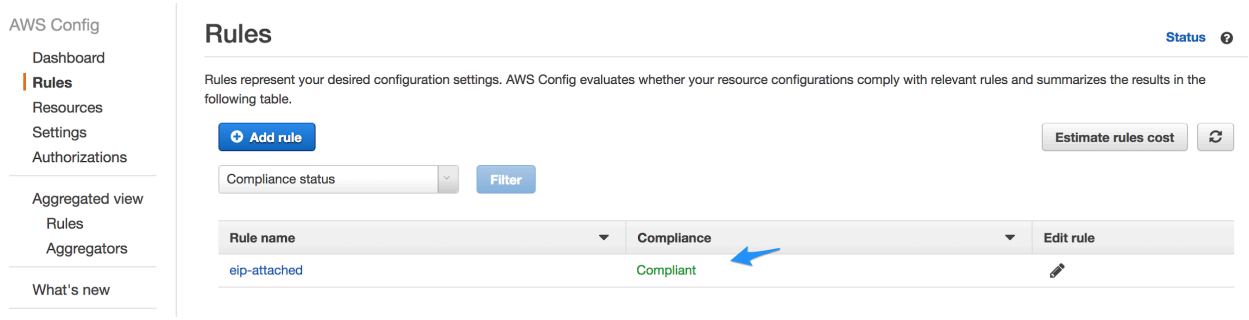
Lets attach this EIP with the EC2 Instance

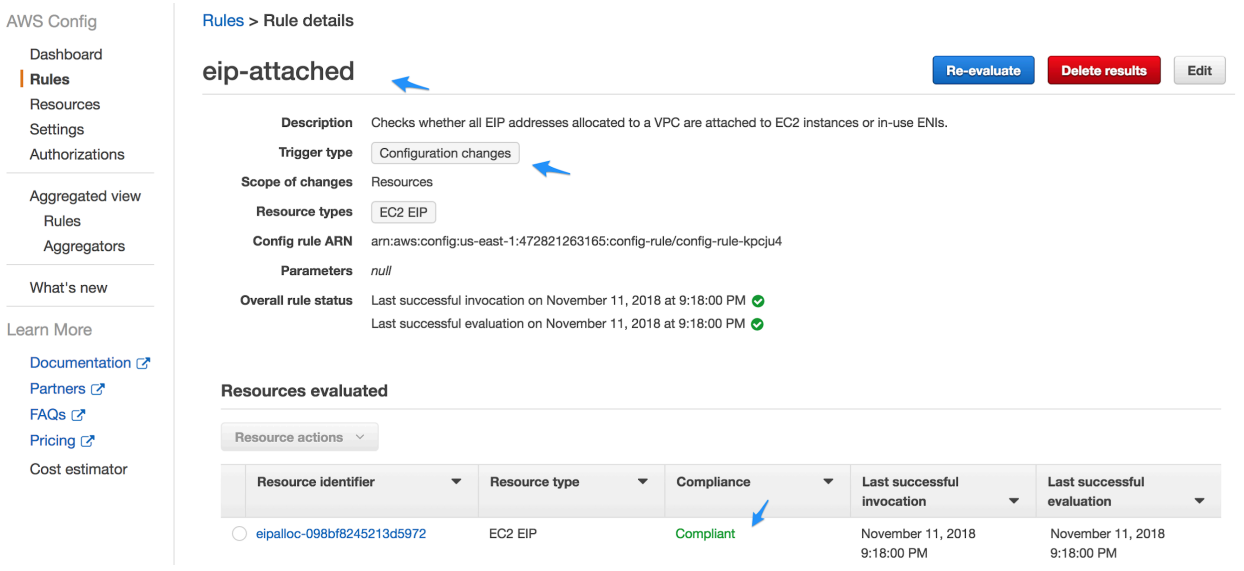


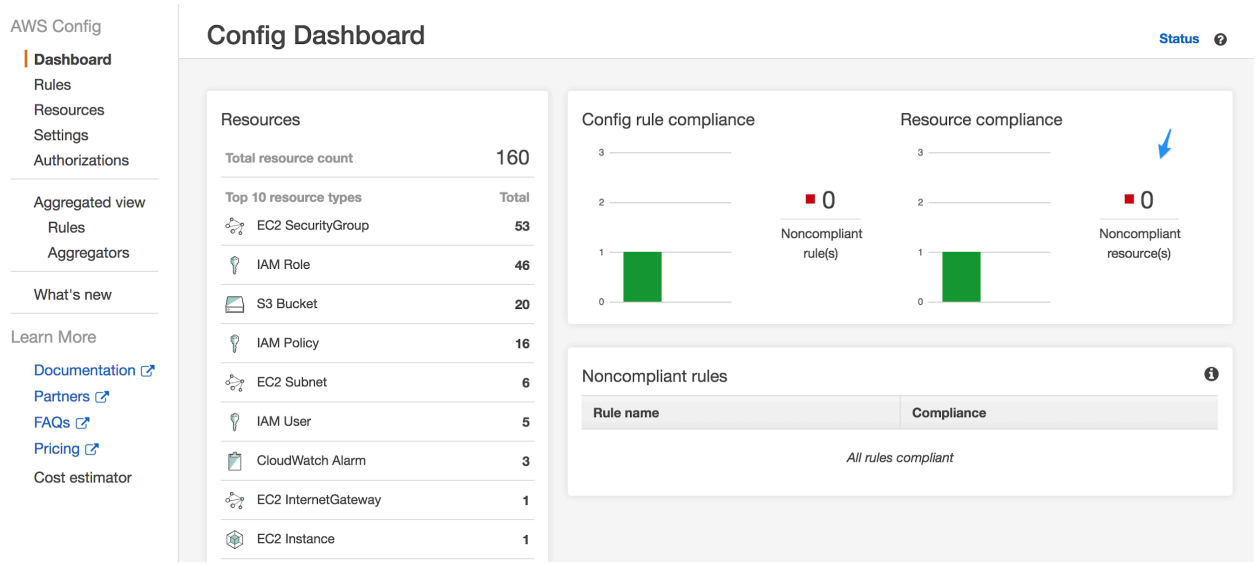

```
INBL2-42RG3QD:~ mahtab.alam$ aws ec2 describe-addresses  --profile mahtab-sysops
{
    "Addresses": [
        {
            "Domain": "vpc",
            "PublicIpv4Pool": "amazon",
            "InstanceId": "i-0f75322c7eab4f14b",
            "NetworkInterfaceId": "eni-0400e391c87abff3a",
            "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

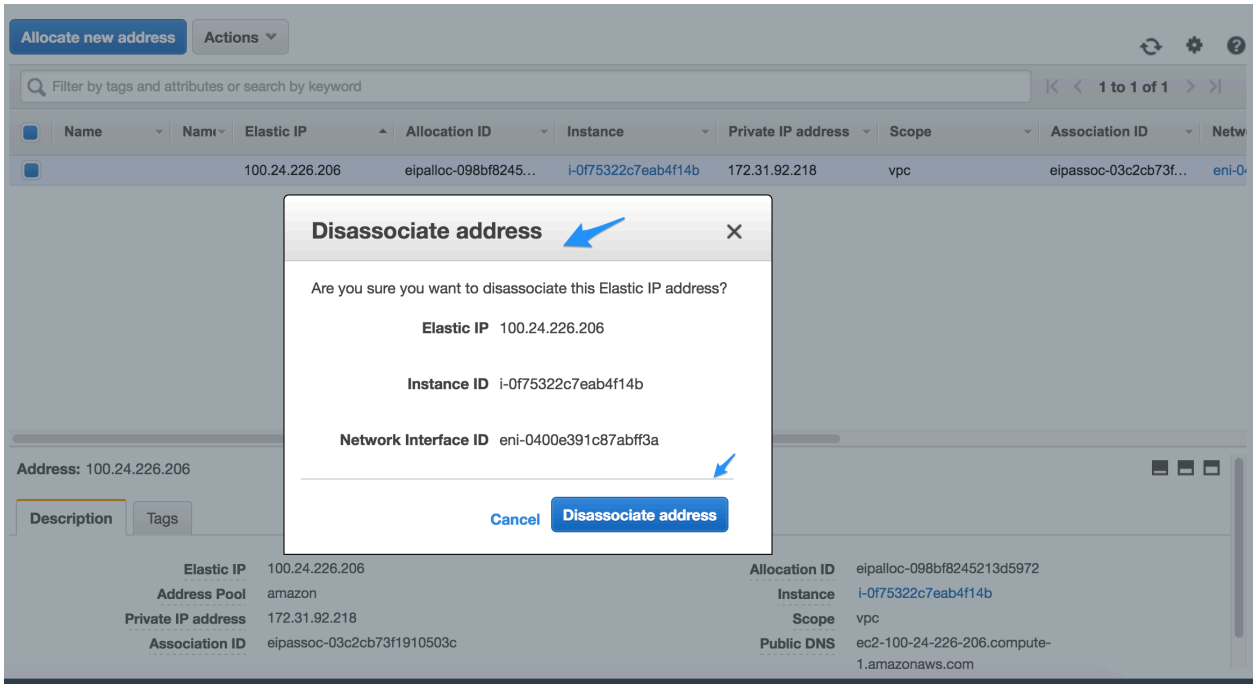

AWS Config
Dashboard
Rules
Resources
Settings
Authorizations
Aggregated view
Rules
Aggregators
What's new
Learn More
Documentation
Partners
FAQs
Pricing
Cost estimator
Rules > Rule details
eip-attached
Re-evaluate
Delete results
Edit
Description
Checks whether all EIP addresses allocated to a VPC are 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
Not available
Lets manually re-evaluate the eip-attached rule
Resources evaluated
Resource actions
Resource identifier
Resource type
Compliance
Last successful invocation
Last successful evaluation


AWS Config
Dashboard
Rules
Resources
Settings
Authorizations
Aggregated view
Rules
Aggregators
What's new
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


AWS Config
Dashboard
Rules
Resources
Settings
Authorizations
Aggregated view
Rules
Aggregators
What's new
Learn More
Documentation
Partners
FAQs
Pricing
Cost estimator
Rules > Rule details
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

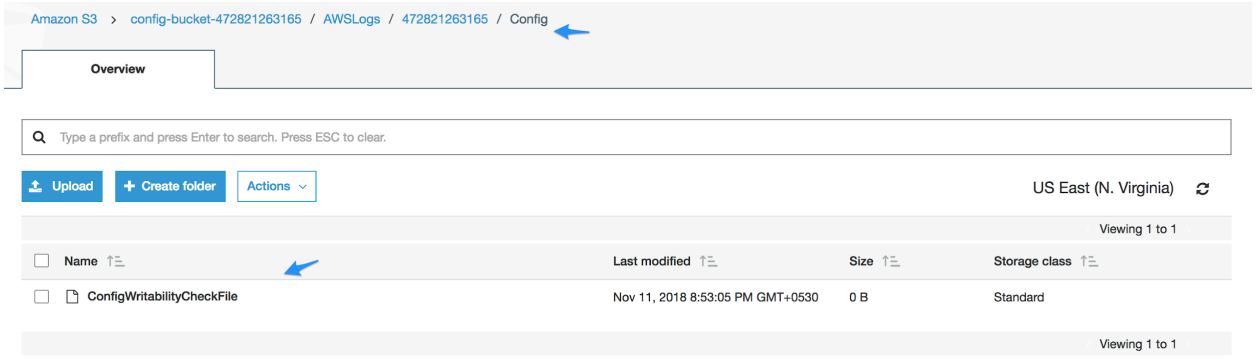


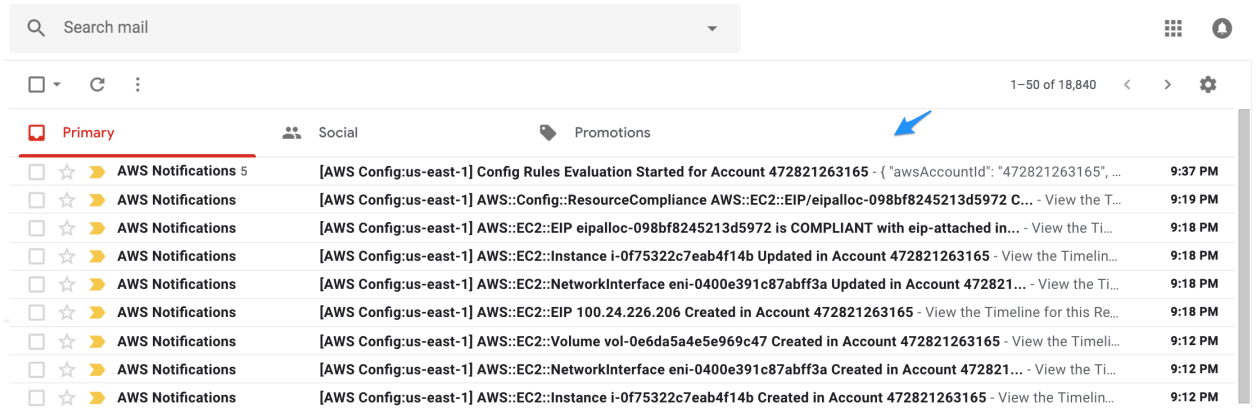
Now lets disassociate the EIP from EC2 Instance

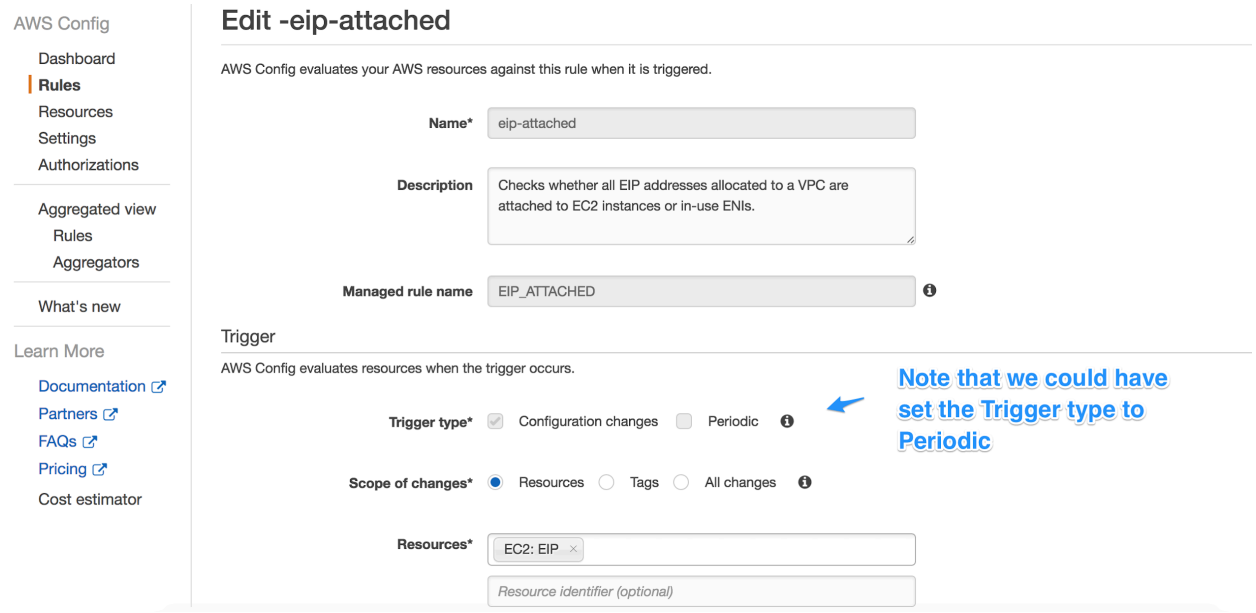


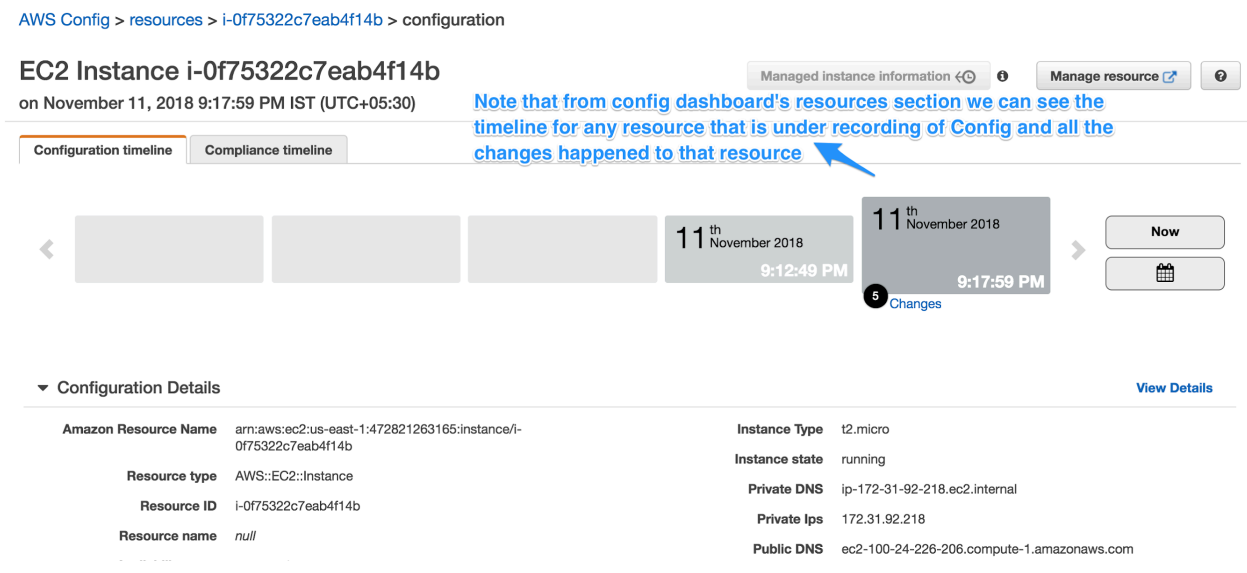
```
INBL2-42RG3QD:~ mahtab.alam$ aws ec2 describe-addresses  --profile mahtab-sysops
{
    "Addresses": [
        {
            "PublicIp": "100.24.226.206",
            "Domain": "vpc",
            "AllocationId": "eipalloc-098bf8245213d5972",
            "PublicIpv4Pool": "amazon"
        }
    ]
}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

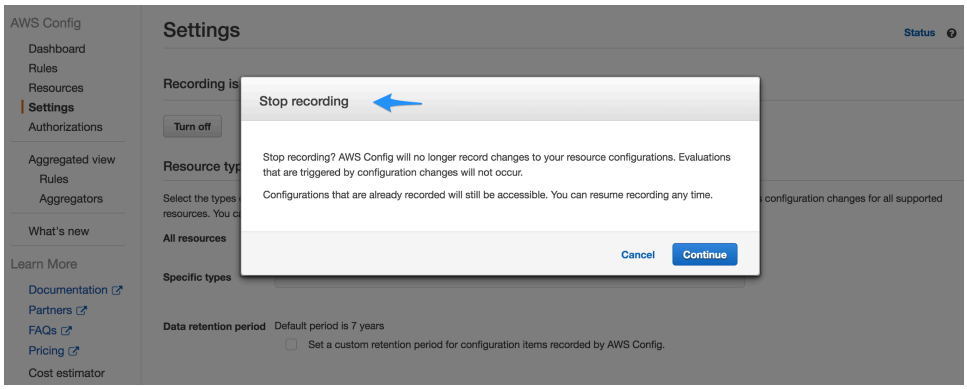
Now our eip-attached rule will show non-compliant for the EIP






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
Note that we could have set the Trigger type to Periodic
Scope of changes*
Resources
Tags
All changes
Resources*
EC2: EIP
Resource identifier (optional)


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
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
Configuration timeline
Compliance timeline
11th November 2018
9:12:49 PM
11th November 2018
9:17:59 PM
5 Changes
Now
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 typ
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