



# Develop Compliant Infrastructure

Isn't it better to prevent non-compliant resources to be deployed in the first place?

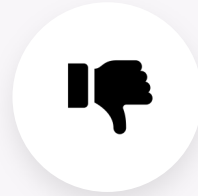


# Who has used AWS Config



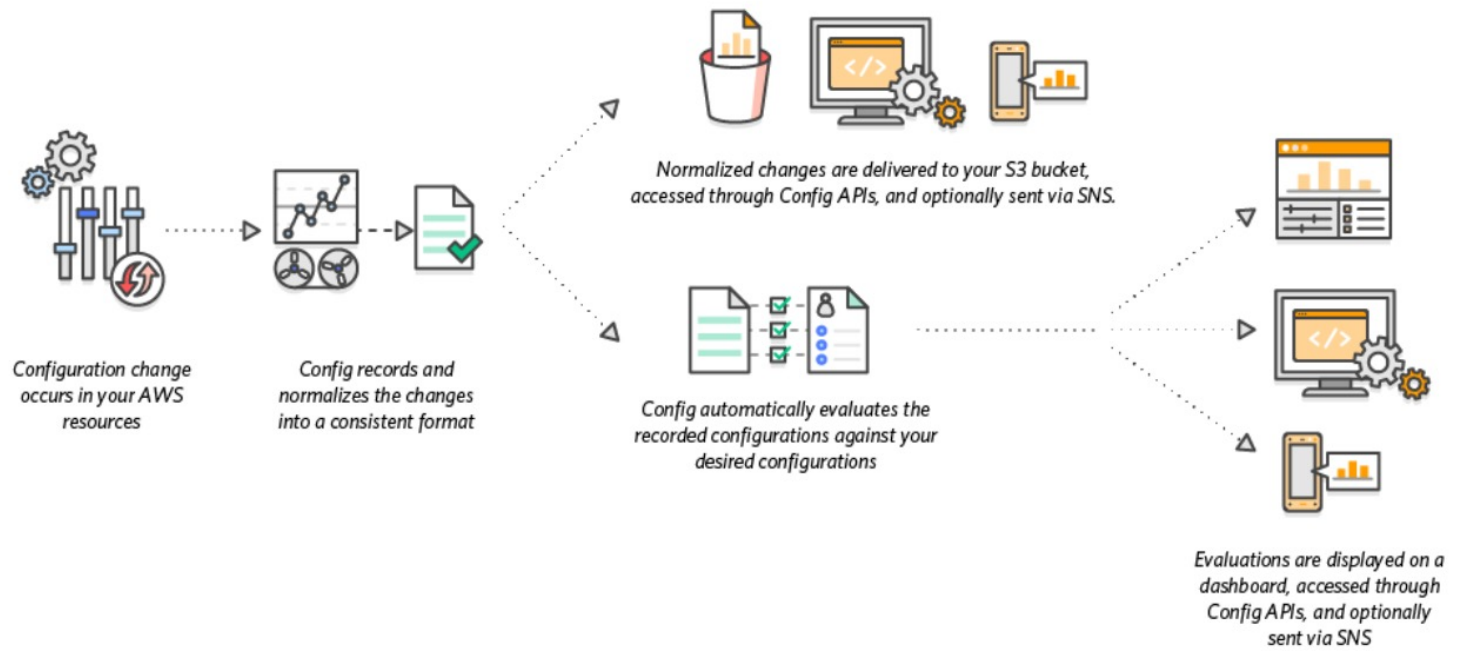
## Thumb Up

Yes, I used AWS Config before



## Thumb Down

No, I did not use AWS Config before



# Rules

AWS Config uses rules



MY SECRET  
PLAN  
TO RULE  
THE WORLD

**What is the  
problem?**





# Who knows cfn-guard



Thumb Up  
Yes, I know it!



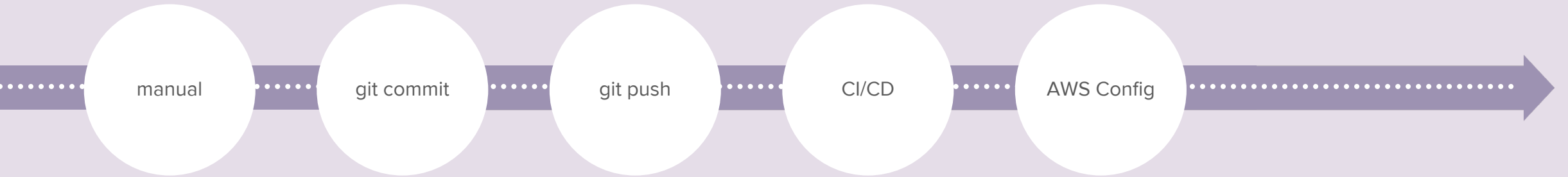
Thumb Down  
No, I do not know it



# CFN Guard

Validate Cloud Environments with Policy-as-Code

# Development lifecycle



# Build AWS Config rules using AWS CloudFormation Guard

Posted On: Aug 2, 2022

AWS Config now supports an easier way to author custom AWS Config rules using AWS CloudFormation Guard ([cfn-guard](#)). With this release, users with limited programming experience can use Guard to define and review custom policies that check your resources have desired configurations. AWS Config rules are a way of creating and implementing compliance policies against resource configurations. Currently, AWS Config offers both managed rules, which AWS builds and maintains to meet common compliance use cases, and custom rules, which users create to meet their specific compliance needs. Guard is an open source tool offering policy-as-code, such that users can define policies to validate JSON- or YAML-formatted data using a domain-specific language (DSL).

Previously, to create a custom rule, you would have to define an AWS Lambda function, typically in languages such as Java or Python. Now, you can author AWS Config custom rules using Guard DSL without needing to develop AWS Lambda functions. Security and compliance administrators have a simpler way to write custom logic which reflects the compliance needs your organization has defined for itself.

To get started, you can use the AWS Config console to create your own AWS Config rule through the 'Add rule' workflow. The rule logic will be validated for correctness prior to deployment such that you do not have to perform error checking for oversized configuration items or deleted resources; Guard also simplifies permissioning to place the rules in your account. As a result, AWS Config rules using Guard removes the complexity of rule authoring, reducing overall development time for rules. Once the rule is deployed, you will be able to view logs of resource compliance status based on your rule evaluations in AWS Config.

AWS Config rules using Guard are available in all commercial [AWS regions](#) and are charged the same as AWS Config rules, which uses a tiered pricing model based on the number of rules evaluations you run each month; there is no additional charge for authoring these rules in Guard. To learn more about authoring AWS Config rules using Guard, see our [documentation](#). To learn more about our pricing, visit the AWS Config [pricing page](#).



# Thank You

Joris Conijn