


































-  Secrets
-  ABAP
-  Apex
-  C
-  C++
-  **CloudFormation**
-  COBOL
-  C#
-  CSS
-  Flex
-  Go
-  HTML
-  Java
-  JavaScript
-  Kotlin
-  Kubernetes
-  Objective C
-  PHP
-  PL/I
-  PL/SQL
-  Python
-  RPG
-  Ruby
-  Scala
-  Swift
-  Terraform
-  Text
-  TypeScript
-  T-SQL
-  VB.NET
-  VB6
-  XML



CloudFormation static code analysis

Unique rules to find Bugs, Vulnerabilities, Security Hotspots, and Code Smells in your CLOUDFORMATION code

All rules 27














 Vulnerability 3

 Security Hotspot 20

 Code Smell 4

Tags ▾

Search by name... 🔍

 Security Hotspot
Using unencrypted SNS topics is security-sensitive 
Using unencrypted SageMaker notebook instances is security-sensitive 
Using unencrypted Elasticsearch domains is security-sensitive 
Using unencrypted RDS databases is security-sensitive 
Using unencrypted EBS volumes is security-sensitive 
Disabling logging is security-sensitive 
"Log Groups" should be declared explicitly 
Administration services access should be restricted to specific IP addresses 
Disabling versioning of S3 buckets is security-sensitive 
Disabling server-side encryption of S3 buckets is security-sensitive 
AWS tag keys should comply with a naming convention 
CloudFormation parsing failure 

"Log Groups" should be declared explicitly

Analyze your code

 Code Smell

 Major ?

 convention aws

Some AWS services create `Log Groups` implicitly and don't let the developer choose the `Log Group` name. This means that CloudFormation does not require the developer to declare the `Log Group` that the resource will write to.

If a `Log Group` is not declared within CloudFormation, then this `Log Group` will be automatically created at run time and it won't be managed by CloudFormation. The consequences are that the:

- `Log Group` will not be removed when the `Stack` is removed.
- `Log Group` attributes (such as retention) won't be managed "as code" within CloudFormation.

These automatically created `Log Groups` will remain forever which can have huge impact on costs and security (the data stay forever while this is unexpected from company or regulatory rules).

A good practice is to declare the target `Log Group` with CloudFormation, matching the name that the AWS will use so that the `Log Group` resource is managed as code.

This rule applies to the following resources:

- `AWS::Lambda::Function`
- `AWS::Serverless::Function`
- `AWS::ApiGatewayV2::Api`
- `AWS::CodeBuild::Project`

Noncompliant Code Example

```
# There is no "Log Group" declared corresponding to "MyLambdaFunction": logs will not be managed
MyLambdaFunction:
  Type: AWS::Lambda::Function
  Properties:
    Runtime: nodejs12.x
    Description: Example of Lambda Function
```

Compliant Solution

Example with Ref

```
MyLambdaFunction:
  Type: AWS::Lambda::Function
  Properties:
    Runtime: nodejs12.x
    Description: Example of Lambda Function

MyFunctionLogGroup:
  Type: AWS::Logs::LogGroup
  Properties:
    LogGroupName: !Join ['/', ['/aws/lambda', !Ref MyLambdaFunction]]
    RetentionInDays: 30
```

Example with Sub

```
MyLambdaFunction:
  Type: AWS::Lambda::Function
  Properties:
    Runtime: nodejs12.x
    Description: Example of Lambda Function

MyFunctionLogGroupSub:
  Type: AWS::Logs::LogGroup
  Properties:
    LogGroupName: !Sub '/aws/lambda/${MyLambdaFunction}'
    RetentionInDays: 30
```

Available In:

 | 