

































-  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... 

Defining a short backup retention duration is security-sensitive		Security Hotspot
Using unencrypted EFS file systems is security-sensitive		Security Hotspot
Using unencrypted SQS queues is security-sensitive		Security Hotspot
Using unencrypted SNS topics is security-sensitive		Security Hotspot
Using unencrypted SageMaker notebook instances is security-sensitive		Security Hotspot
Using unencrypted Elasticsearch domains is security-sensitive		Security Hotspot
Using unencrypted RDS databases is security-sensitive		Security Hotspot
Using unencrypted EBS volumes is security-sensitive		Security Hotspot
Disabling logging is security-sensitive		Security Hotspot
"Log Groups" should be declared explicitly		Code Smell
Administration services access should be restricted to specific IP addresses		Vulnerability
Disabling versioning of S3 buckets is security-sensitive		Security Hotspot
Disabling server-side encryption of S3 buckets is security-sensitive		

Defining a short backup retention duration is security-sensitive

Analyze your code

 Security Hotspot

 Major 

 aws

Reducing the backup retention duration can reduce an organization's ability to re-establish service in case of a security incident.

Data backups allow to overcome corruption or unavailability of data by recovering as efficiently as possible from a security incident.

Backup retention duration, coverage, and backup locations are essential criteria regarding functional continuity.

Ask Yourself Whether

- This component is essential for the information system infrastructure.
- This component is essential for mission-critical functions.
- Compliance policies require this component to be backed up for a specific amount of time.

There is a risk if you answered yes to any of those questions.

Recommended Secure Coding Practices

Increase the backup retention period to an amount of time sufficient enough to be able to restore service in case of an incident.

Sensitive Code Example

For [Amazon Relational Database Service](#) clusters and instances:

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  relationaldatabase:
    Type: 'AWS::RDS::DBInstance'
    Properties:
      DBName: NonCompliantDatabase
      BackupRetentionPeriod: 2 # Sensitive
```

Compliant Solution

For [Amazon Relational Database Service](#) clusters and instances:

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  relationaldatabase:
    Type: 'AWS::RDS::DBInstance'
    Properties:
      DBName: CompliantDatabase
      BackupRetentionPeriod: 5
```

Available In: