**CloudFormation static code analysis**

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

### [Creating public APIs is security-sensitive](https://rules.sonarsource.com/cloudformation/RSPEC-6333)

[Security Hotspot](https://rules.sonarsource.com/cloudformation/RSPEC-6333)

### [Allowing public network access to cloud resources is security-sensitive](https://rules.sonarsource.com/cloudformation/RSPEC-6329)

[Security Hotspot](https://rules.sonarsource.com/cloudformation/RSPEC-6329)

### [Having AWS policies that grant access to all resources of an account is security-sensitive](https://rules.sonarsource.com/cloudformation/RSPEC-6304)

[Security Hotspot](https://rules.sonarsource.com/cloudformation/RSPEC-6304)

### [Having policies that grant all privileges is security-sensitive](https://rules.sonarsource.com/cloudformation/RSPEC-6302)

[Security Hotspot](https://rules.sonarsource.com/cloudformation/RSPEC-6302)

### [Policies authorizing public access to resources are security-sensitive](https://rules.sonarsource.com/cloudformation/RSPEC-6270)

[Security Hotspot](https://rules.sonarsource.com/cloudformation/RSPEC-6270)

### [Granting access to S3 buckets to all or authenticated users is security-sensitive](https://rules.sonarsource.com/cloudformation/RSPEC-6265)

[Security Hotspot](https://rules.sonarsource.com/cloudformation/RSPEC-6265)

### [AWS IAM policies should not allow privilege escalation](https://rules.sonarsource.com/cloudformation/RSPEC-6317)

[Vulnerability](https://rules.sonarsource.com/cloudformation/RSPEC-6317)

### [Weak SSL/TLS protocols should not be used](https://rules.sonarsource.com/cloudformation/RSPEC-4423)

[Vulnerability](https://rules.sonarsource.com/cloudformation/RSPEC-4423)

### [Allowing public ACLs or policies on a S3 bucket is security-sensitive](https://rules.sonarsource.com/cloudformation/RSPEC-6281)

[Security Hotspot](https://rules.sonarsource.com/cloudformation/RSPEC-6281)

### [Authorizing HTTP communications with S3 buckets is security-sensitive](https://rules.sonarsource.com/cloudformation/RSPEC-6249)

[Security Hotspot](https://rules.sonarsource.com/cloudformation/RSPEC-6249)

### [Using clear-text protocols is security-sensitive](https://rules.sonarsource.com/cloudformation/RSPEC-5332)

[Security Hotspot](https://rules.sonarsource.com/cloudformation/RSPEC-5332)

### ["Log Groups" should be configured with a retention policy](https://rules.sonarsource.com/cloudformation/RSPEC-6295)

[Code Smell](https://rules.sonarsource.com/cloudformation/RSPEC-6295)

### [Defining a short backup retention duration is security-sensitive](https://rules.sonarsource.com/cloudformation/RSPEC-6364)

[Security Hotspot](https://rules.sonarsource.com/cloudformation/RSPEC-6364)

### [Using unencrypted EFS file systems is security-sensitive](https://rules.sonarsource.com/cloudformation/RSPEC-6332)

[Security Hotspot](https://rules.sonarsource.com/cloudformation/RSPEC-6332)

### [Using unencrypted SQS queues is security-sensitive](https://rules.sonarsource.com/cloudformation/RSPEC-6330)

[Security Hotspot](https://rules.sonarsource.com/cloudformation/RSPEC-6330)

### [Using unencrypted SNS topics is security-sensitive](https://rules.sonarsource.com/cloudformation/RSPEC-6327)

[Security Hotspot](https://rules.sonarsource.com/cloudformation/RSPEC-6327)

### [Using unencrypted SageMaker notebook instances is security-sensitive](https://rules.sonarsource.com/cloudformation/RSPEC-6319)

[Security Hotspot](https://rules.sonarsource.com/cloudformation/RSPEC-6319)

### [Using unencrypted Elasticsearch domains is security-sensitive](https://rules.sonarsource.com/cloudformation/RSPEC-6308)

[Security Hotspot](https://rules.sonarsource.com/cloudformation/RSPEC-6308)

### [Using unencrypted RDS databases is security-sensitive](https://rules.sonarsource.com/cloudformation/RSPEC-6303)

[Security Hotspot](https://rules.sonarsource.com/cloudformation/RSPEC-6303)

### [Using unencrypted EBS volumes is security-sensitive](https://rules.sonarsource.com/cloudformation/RSPEC-6275)

[Security Hotspot](https://rules.sonarsource.com/cloudformation/RSPEC-6275)

### [Disabling logging is security-sensitive](https://rules.sonarsource.com/cloudformation/RSPEC-6258)

[Security Hotspot](https://rules.sonarsource.com/cloudformation/RSPEC-6258)

### ["Log Groups" should be declared explicitly](https://rules.sonarsource.com/cloudformation/RSPEC-6294)

[Code Smell](https://rules.sonarsource.com/cloudformation/RSPEC-6294)

### [Administration services access should be restricted to specific IP addresses](https://rules.sonarsource.com/cloudformation/RSPEC-6321)

[Vulnerability](https://rules.sonarsource.com/cloudformation/RSPEC-6321)

### [Disabling versioning of S3 buckets is security-sensitive](https://rules.sonarsource.com/cloudformation/RSPEC-6252)

[Security Hotspot](https://rules.sonarsource.com/cloudformation/RSPEC-6252)

### [Disabling server-side encryption of S3 buckets is security-sensitive](https://rules.sonarsource.com/cloudformation/RSPEC-6245)

[Security Hotspot](https://rules.sonarsource.com/cloudformation/RSPEC-6245)

### [AWS tag keys should comply with a naming convention](https://rules.sonarsource.com/cloudformation/RSPEC-6273)

[Code Smell](https://rules.sonarsource.com/cloudformation/RSPEC-6273)

### [CloudFormation parsing failure](https://rules.sonarsource.com/cloudformation/RSPEC-2260)

[Code Smell](https://rules.sonarsource.com/cloudformation/RSPEC-2260)