CloudFormation static code analysis

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

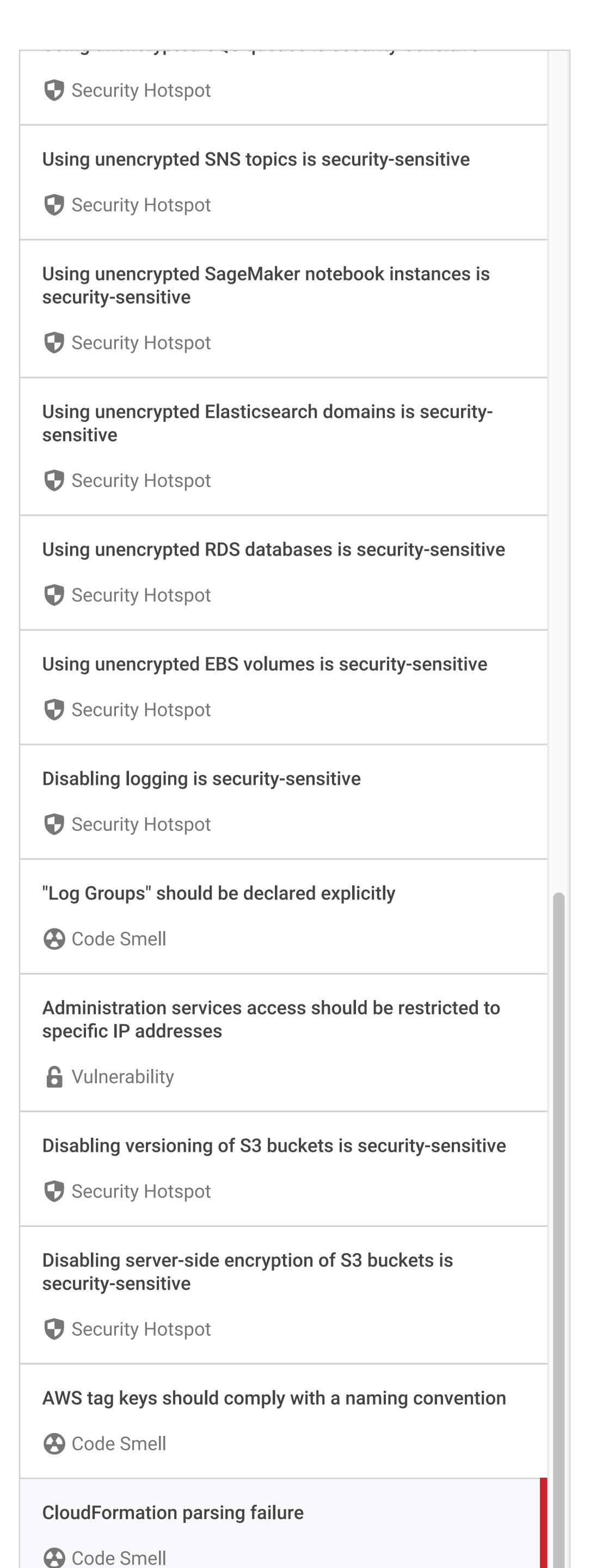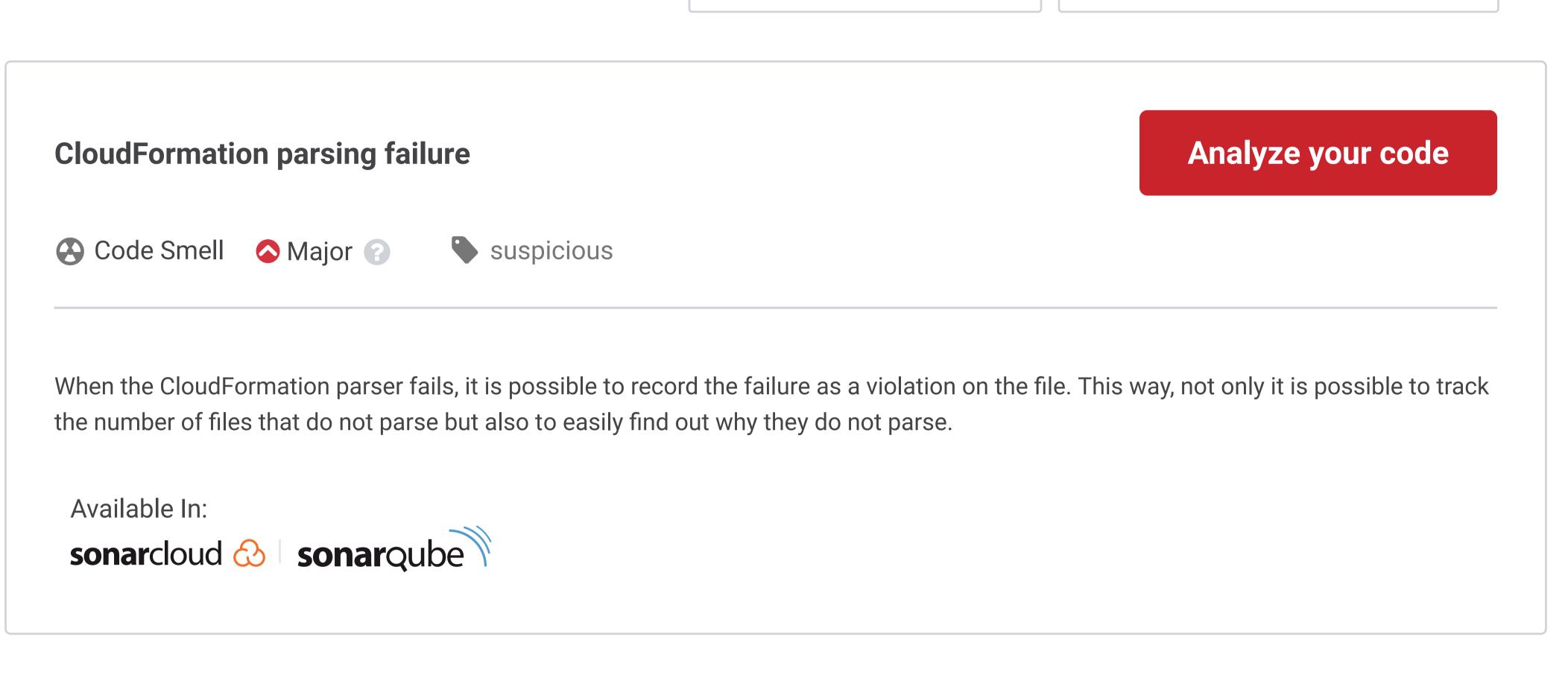|		
Secrets		
ABAP		
Apex		
C		
C++		
CloudFormation		
COBOL		
C#		
CSS		
Flex		
Go		
HTML		
Java		
JavaScript		
Kotlin		
Kubernetes		
Objective C		
PHP		
PL/I		
PL/SQL		
Python		
RPG		
Ruby		
Scala		
Swift		
Terraform		
Text		
TypeScript		
T-SQL		
VB.NET		
VB6		
XML		

All rules 27 | 🔒 Vulnerability ③ | 🛡 Security Hotspot ⑳ | ☢ Code Smell ④

Tags ⌄ | Search by name... 🔍

🛡 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

🛡 Security Hotspot

AWS tag keys should comply with a naming convention

☢ Code Smell

CloudFormation parsing failure

☢ Code Smell

CloudFormation parsing failure

Analyze your code

☢ Code Smell   ⬆ Major ⓘ   🏷 suspicious

When the CloudFormation parser fails, it is possible to record the failure as a violation on the file. This way, not only it is possible to track the number of files that do not parse but also to easily find out why they do not parse.

Available In:

sonarcloud ☁ | **sonar**qube