## Terraform static code analysis

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[Google Cloud load balancers SSL policies should not offer weak cipher suites](https://rules.sonarsource.com/terraform/RSPEC-6410)

[Vulnerability](https://rules.sonarsource.com/terraform/RSPEC-6410)

[Azure custom roles should not grant subscription Owner capabilities](https://rules.sonarsource.com/terraform/RSPEC-6385)

[Vulnerability](https://rules.sonarsource.com/terraform/RSPEC-6385)

[Excluding users or groups activities from audit logs is security-sensitive](https://rules.sonarsource.com/terraform/RSPEC-6414)

[Security Hotspot](https://rules.sonarsource.com/terraform/RSPEC-6414)

[Defining a short log retention duration is security-sensitive](https://rules.sonarsource.com/terraform/RSPEC-6413)

[Security Hotspot](https://rules.sonarsource.com/terraform/RSPEC-6413)

[Enabling Attribute-Based Access Control for Kubernetes is security-sensitive](https://rules.sonarsource.com/terraform/RSPEC-6409)

[Security Hotspot](https://rules.sonarsource.com/terraform/RSPEC-6409)

[Creating custom roles allowing privilege escalation is security-sensitive](https://rules.sonarsource.com/terraform/RSPEC-6408)

[Security Hotspot](https://rules.sonarsource.com/terraform/RSPEC-6408)

[Creating App Engine handlers without requiring TLS is security-sensitive](https://rules.sonarsource.com/terraform/RSPEC-6407)

[Security Hotspot](https://rules.sonarsource.com/terraform/RSPEC-6407)

[Excessive granting of GCP IAM permissions is security-sensitive](https://rules.sonarsource.com/terraform/RSPEC-6406)

[Security Hotspot](https://rules.sonarsource.com/terraform/RSPEC-6406)

[Enabling project-wide SSH keys to access VM instances is security-sensitive](https://rules.sonarsource.com/terraform/RSPEC-6405)

[Security Hotspot](https://rules.sonarsource.com/terraform/RSPEC-6405)

[Granting public access to GCP resources is security-sensitive](https://rules.sonarsource.com/terraform/RSPEC-6404)

[Security Hotspot](https://rules.sonarsource.com/terraform/RSPEC-6404)

[Creating GCP SQL instances without requiring TLS is security-sensitive](https://rules.sonarsource.com/terraform/RSPEC-6403)

[Security Hotspot](https://rules.sonarsource.com/terraform/RSPEC-6403)

[Creating DNS zones without DNSSEC enabled is security-sensitive](https://rules.sonarsource.com/terraform/RSPEC-6402)

[Security Hotspot](https://rules.sonarsource.com/terraform/RSPEC-6402)

[Creating keys without a rotation period is security-sensitive](https://rules.sonarsource.com/terraform/RSPEC-6401)

[Security Hotspot](https://rules.sonarsource.com/terraform/RSPEC-6401)

[Granting highly privileged GCP resource rights is security-sensitive](https://rules.sonarsource.com/terraform/RSPEC-6400)

[Security Hotspot](https://rules.sonarsource.com/terraform/RSPEC-6400)

[Using unencrypted cloud storages is security-sensitive](https://rules.sonarsource.com/terraform/RSPEC-6388)

[Security Hotspot](https://rules.sonarsource.com/terraform/RSPEC-6388)

[Azure role assignments that grant access to all resources of a subscription are security-sensitive](https://rules.sonarsource.com/terraform/RSPEC-6387)

[Security Hotspot](https://rules.sonarsource.com/terraform/RSPEC-6387)

[Disabling Role-Based Access Control on Azure resources is security-sensitive](https://rules.sonarsource.com/terraform/RSPEC-6383)

[Security Hotspot](https://rules.sonarsource.com/terraform/RSPEC-6383)

[Disabling certificate-based authentication is security-sensitive](https://rules.sonarsource.com/terraform/RSPEC-6382)

[Security Hotspot](https://rules.sonarsource.com/terraform/RSPEC-6382)

[Assigning high privileges Azure Resource Manager built-in roles is security-sensitive](https://rules.sonarsource.com/terraform/RSPEC-6381)

[Security Hotspot](https://rules.sonarsource.com/terraform/RSPEC-6381)

[Authorizing anonymous access to Azure resources is security-sensitive](https://rules.sonarsource.com/terraform/RSPEC-6380)

[Security Hotspot](https://rules.sonarsource.com/terraform/RSPEC-6380)

[Enabling Azure resource-specific admin accounts is security-sensitive](https://rules.sonarsource.com/terraform/RSPEC-6379)

[Security Hotspot](https://rules.sonarsource.com/terraform/RSPEC-6379)

[Disabling Managed Identities for Azure resources is security-sensitive](https://rules.sonarsource.com/terraform/RSPEC-6378)

[Security Hotspot](https://rules.sonarsource.com/terraform/RSPEC-6378)

[Assigning high privileges Azure Active Directory built-in roles is security-sensitive](https://rules.sonarsource.com/terraform/RSPEC-6375)

[Security Hotspot](https://rules.sonarsource.com/terraform/RSPEC-6375)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[Unversioned Google Cloud Storage buckets are security-sensitive](https://rules.sonarsource.com/terraform/RSPEC-6412)

[Security Hotspot](https://rules.sonarsource.com/terraform/RSPEC-6412)

[Disabling S3 bucket MFA delete is security-sensitive](https://rules.sonarsource.com/terraform/RSPEC-6255)

[Security Hotspot](https://rules.sonarsource.com/terraform/RSPEC-6255)

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

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

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

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

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

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

[Terraform parsing failure](https://rules.sonarsource.com/terraform/RSPEC-2260)

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