

## KICS REPORT

v2.1.3

| CRITICAL | 0 | HIGH | 6 | MEDIUM | 9 | LOW | 6 | INFO | 33 | TOTAL | 54 |
|----------|---|------|---|--------|---|-----|---|------|----|-------|----|
|----------|---|------|---|--------|---|-----|---|------|----|-------|----|

PLATFORMS Terraform  
START TIME 13:48:20, Dec 12 2024  
END TIME 13:48:34, Dec 12 2024  
SCANNED PATHS:  
- /path

### 🛡️ DynamoDB Table Not Encrypted

Results 1

Severity HIGH  
Platform Terraform  
Cwe 311  
Category Encryption

#### Description

AWS DynamoDB Tables should have server-side encryption

```
../../../../path/remote-backend/main.tf:11
```

Expected: aws\_dynamodb\_table.server\_side\_encryption.enabled should be set to true

### 🛡️ S3 Bucket Allows Public Policy

Results 1

Severity HIGH  
Platform Terraform  
Cwe 284  
Category Access Control

#### Description

S3 bucket allows public policy

```
../../../../path/main.tf:15
```

Expected: 'block\_public\_policy' should equal 'true'

### 🛡️ Sensitive Port Is Exposed To Entire Network

Results 2

Severity HIGH  
Platform Terraform  
Cwe 200  
Category Networking and Firewall

#### Description

A sensitive port, such as port 23 or port 110, is open for the whole network in either TCP or UDP protocol

```
../../../../path/security-groups/main.tf:3
```

Expected: SSH (TCP:22) should not be allowed

```
../../../../path/security-groups/main.tf:3
```

Expected: HTTPS (TCP:443) should not be allowed

### 🛡️ Unrestricted Security Group Ingress

Results 2

Severity HIGH  
Platform Terraform  
Cwe 668  
Category Networking and Firewall

#### Description

Security groups allow ingress from 0.0.0.0:0 and/or ::/0

<https://kics.io>

## KICS REPORT

v2.1.3

..../path/security-groups/main.tf:7

Expected: One of 'ingress.cidr\_blocks' not equal '0.0.0.0/0'

..../path/security-groups/main.tf:13

Expected: One of 'ingress.cidr\_blocks' not equal '0.0.0.0/0'

### 🛡 EC2 Instance Has Public IP

Results

1

Severity MEDIUM

Platform Terraform

Cwe 200

Category Networking and Firewall

#### Description

EC2 Instance should not have a public IP address.

..../path/ec2/main.tf:1

Expected: 'associate\_public\_ip\_address' should be defined and not null

### 🛡 EC2 Instance Monitoring Disabled

Results

1

Severity MEDIUM

Platform Terraform

Cwe 778

Category Observability

#### Description

EC2 Instance should have detailed monitoring enabled. With detailed monitoring enabled data is available in 1-minute periods

..../path/ec2/main.tf:1

Expected: 'monitoring' should be defined and not null

### 🛡 S3 Bucket Allows Public ACL

Results

1

Severity MEDIUM

Platform Terraform

Cwe 284

Category Access Control

#### Description

S3 bucket allows public ACL

..../path/main.tf:15

Expected: 'block\_public\_acls' should equal 'true'

### 🛡 S3 Bucket Logging Disabled

Results

2

Severity MEDIUM

Platform Terraform

Cwe 778

Category Observability

#### Description

Server Access Logging should be enabled on S3 Buckets so that all changes are logged and trackable

..../path/remote-backend/main.tf:1

Expected: 'logging' should be defined and not null

..../path/main.tf:15

<https://kics.io>

## KICS REPORT

v2.1.3

Expected: 'logging' should be defined and not null

### 🛡 S3 Bucket Without Ignore Public ACL

Results

1

|          |                         |
|----------|-------------------------|
| Severity | MEDIUM                  |
| Platform | Terraform               |
| Cwe      | 284                     |
| Category | Insecure Configurations |

#### Description

S3 bucket without ignore public ACL

..../path/main.tf:15

Expected: 'ignore\_public\_acls' should equal 'true'

### 🛡 S3 Bucket Without Restriction Of Public Bucket

Results

1

|          |                         |
|----------|-------------------------|
| Severity | MEDIUM                  |
| Platform | Terraform               |
| Cwe      | 284                     |
| Category | Insecure Configurations |

#### Description

S3 bucket without restriction of public bucket

..../path/main.tf:15

Expected: 'restrict\_public\_buckets' should equal 'true'

### 🛡 S3 Bucket Without Versioning

Results

1

|          |           |
|----------|-----------|
| Severity | MEDIUM    |
| Platform | Terraform |
| Cwe      | 710       |
| Category | Backup    |

#### Description

S3 bucket should have versioning enabled

..../path/main.tf:15

Expected: 'versioning' should be true

### 🛡 Security Group With Unrestricted Access To SSH

Results

1

|          |                         |
|----------|-------------------------|
| Severity | MEDIUM                  |
| Platform | Terraform               |
| Cwe      | 732                     |
| Category | Networking and Firewall |

#### Description

'SSH' (TCP:22) should not be public in AWS Security Group

..../path/security-groups/main.tf:7

Expected: aws\_security\_group[ec2\_secgroup] 'SSH' (Port:22) should not be public

### 🛡 IAM Access Analyzer Not Enabled

Results

5

|          |           |
|----------|-----------|
| Severity | LOW       |
| Platform | Terraform |
| Cwe      | 710       |

## KICS REPORT

v2.1.3

Category Best Practices

### Description

IAM Access Analyzer should be enabled and configured to continuously monitor resource permissions

```
../../path/remote-backend/main.tf:1
```

Expected: 'aws\_accessanalyzer\_analyzer' should be set

```
../../path/ec2/main.tf:1
```

Expected: 'aws\_accessanalyzer\_analyzer' should be set

```
../../path/ssh-key/main.tf:1
```

Expected: 'aws\_accessanalyzer\_analyzer' should be set

```
../../path/security-groups/main.tf:1
```

Expected: 'aws\_accessanalyzer\_analyzer' should be set

```
../../path/partial-config/main.tf:1
```

Expected: 'aws\_accessanalyzer\_analyzer' should be set



### S3 Bucket Without Enabled MFA Delete

Results

1

Severity LOW

Platform Terraform

Cwe 710

Category Insecure Configurations

### Description

S3 bucket without MFA Delete Enabled. MFA delete cannot be enabled through Terraform, it can be done by adding a MFA device ([https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_credentials\\_mfa\\_enable.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable.html)) and enabling versioning and MFA delete by using AWS CLI: `aws s3api put-bucket-versioning --versioning-configuration>Status=Enabled,MFADelete=Enabled --bucket=<BUCKET_NAME> --mfa=<MFA_SERIAL_NUMBER>`. Please, also notice that MFA delete can not be used with lifecycle configurations

```
../../path/remote-backend/main.tf:24
```

Expected: 'versioning\_configuration.mfa\_delete' should be defined and not null



### DynamoDB Table Point In Time Recovery Disabled

Results

1

Severity INFO

Platform Terraform

Cwe 754

Category Best Practices

### Description

It's considered a best practice to have point in time recovery enabled for DynamoDB Table

```
../../path/remote-backend/main.tf:11
```

Expected: aws\_dynamodb\_table.point\_in\_time\_recovery.enabled should be enabled



### Name Is Not Snake Case

Results

4

Severity INFO

Platform Terraform

Cwe 710

Category Best Practices

### Description

All names should follow snake case pattern.

```
../../path/main.tf:21
```

Expected: All names should be on snake case pattern

<https://kics.io>

## KICS REPORT

v2.1.3

..../path/main.tf:11

Expected: All names should be on snake case pattern

..../path/main.tf:28

Expected: All names should be on snake case pattern

..../path/main.tf:15

Expected: All names should be on snake case pattern

### 🛡 Output Without Description

Results

6

|          |                |
|----------|----------------|
| Severity | INFO           |
| Platform | Terraform      |
| Cwe      | 710            |
| Category | Best Practices |

#### Description

All outputs should contain a valid description.

..../path/remote-backend/output.tf:1

Expected: 'description' should be defined and not null

..../path/output.tf:6

Expected: 'description' should be defined and not null

..../path/ssh-key/output.tf:1

Expected: 'description' should be defined and not null

..../path/output.tf:10

Expected: 'description' should be defined and not null

..../path/remote-backend/output.tf:5

Expected: 'description' should be defined and not null

..../path/security-groups/output.tf:1

Expected: 'description' should be defined and not null

### 🛡 Resource Not Using Tags

Results

5

|          |                |
|----------|----------------|
| Severity | INFO           |
| Platform | Terraform      |
| Cwe      | 665            |
| Category | Best Practices |

#### Description

AWS services resource tags are an essential part of managing components. As a best practice, the field 'tags' should have additional tags defined other than 'Name'

..../path/ec2/main.tf:7

Expected: aws\_instance[{{ec2\_instances}}].tags has additional tags defined other than 'Name'

..../path/remote-backend/main.tf:1

Expected: aws\_s3\_bucket[{{s3\_state}}].tags should be defined and not null

..../path/security-groups/main.tf:1

Expected: aws\_security\_group[{{ec2\_secgroup}}].tags should be defined and not null

..../path/ssh-key/main.tf:11

Expected: aws\_key\_pair[{{sshkey}}].tags should be defined and not null

..../path/remote-backend/main.tf:11

Expected: aws\_dynamodb\_table[{{s3\_locks}}].tags should be defined and not null

# KICS REPORT

v2.1.3

## 🛡 Security Group Not Used

Results

1

|          |                |
|----------|----------------|
| Severity | INFO           |
| Platform | Terraform      |
| Cwe      | 284            |
| Category | Access Control |

### Description

Security group must be used or not declared

```
..../path/security-groups/main.tf:1  
Expected: 'aws_security_group[ec2_secgroup]' should be used
```

## 🛡 Security Group Rule Without Description

Results

1

|          |                |
|----------|----------------|
| Severity | INFO           |
| Platform | Terraform      |
| Cwe      | 710            |
| Category | Best Practices |

### Description

It's considered a best practice for AWS Security Group to have a description

```
..../path/security-groups/main.tf:1  
Expected: aws_security_group[{{ec2_secgroup}}].description should be defined and not null
```

## 🛡 Security Group Rule Without Description

Results

3

|          |           |
|----------|-----------|
| Severity | INFO      |
| Platform | Terraform |
| Cwe      | 710       |

### Description

It's considered a best practice for all rules in AWS Security Group to have a description

```
..../path/security-groups/main.tf:9  
Expected: aws_security_group[{{ec2_secgroup}}].ingress.description should be defined and not null
```

```
..../path/security-groups/main.tf:3  
Expected: aws_security_group[{{ec2_secgroup}}].ingress.description should be defined and not null
```

```
..../path/security-groups/main.tf:15  
Expected: aws_security_group[{{ec2_secgroup}}].egress.description should be defined and not null
```

## 🛡 Variable Without Description

Results

8

|          |                |
|----------|----------------|
| Severity | INFO           |
| Platform | Terraform      |
| Cwe      | 710            |
| Category | Best Practices |

### Description

All variables should contain a valid description.

```
..../path/security-groups/variables.tf:1  
Expected: 'description' should be defined and not null  
..../path/remote-backend/variables.tf:6
```

## KICS REPORT

v2.1.3

Expected: 'description' should be defined and not null

../../path/partial-config/variables.tf:11

Expected: 'description' should be defined and not null

../../path/remote-backend/variables.tf:1

Expected: 'description' should be defined and not null

../../path/partial-config/variables.tf:1

Expected: 'description' should be defined and not null

../../path/security-groups/variables.tf:5

Expected: 'description' should be defined and not null

../../path/ec2/variables.tf:19

Expected: 'description' should be defined and not null

../../path/partial-config/variables.tf:6

Expected: 'description' should be defined and not null

### 🛡 Variable Without Type

Results

4

Severity INFO

Platform Terraform

Cwe 710

Category Best Practices

#### Description

All variables should contain a valid type.

../../path/security-groups/variables.tf:5

Expected: 'type' should be defined and not null

../../path/ec2/variables.tf:19

Expected: 'type' should be defined and not null

../../path/variables.tf:1

Expected: 'type' should be defined and not null

../../path/security-groups/variables.tf:1

Expected: 'type' should be defined and not null