DevSecOps
containers, vulnerabilities and SCA

OWASP Ottawa
November 2023

Hi, I’m Greg.

DevSecOps chap at Rewind.

greg.sienkiewicz@owasp.org
github.com/gregsienkiewicz

Protect your mission-critical SaaS data now

On-demand backup & restoration for people who manage data security and business continuity.

- Safeguard your IP with automated cloud data backups
- Recover quickly from simple and complex data mistakes
- SOC 2, SOC 3, GDPR, CCPA compliant (see full security reports)
- Mitigate the risk of data loss and downtime
- Restore data in minutes

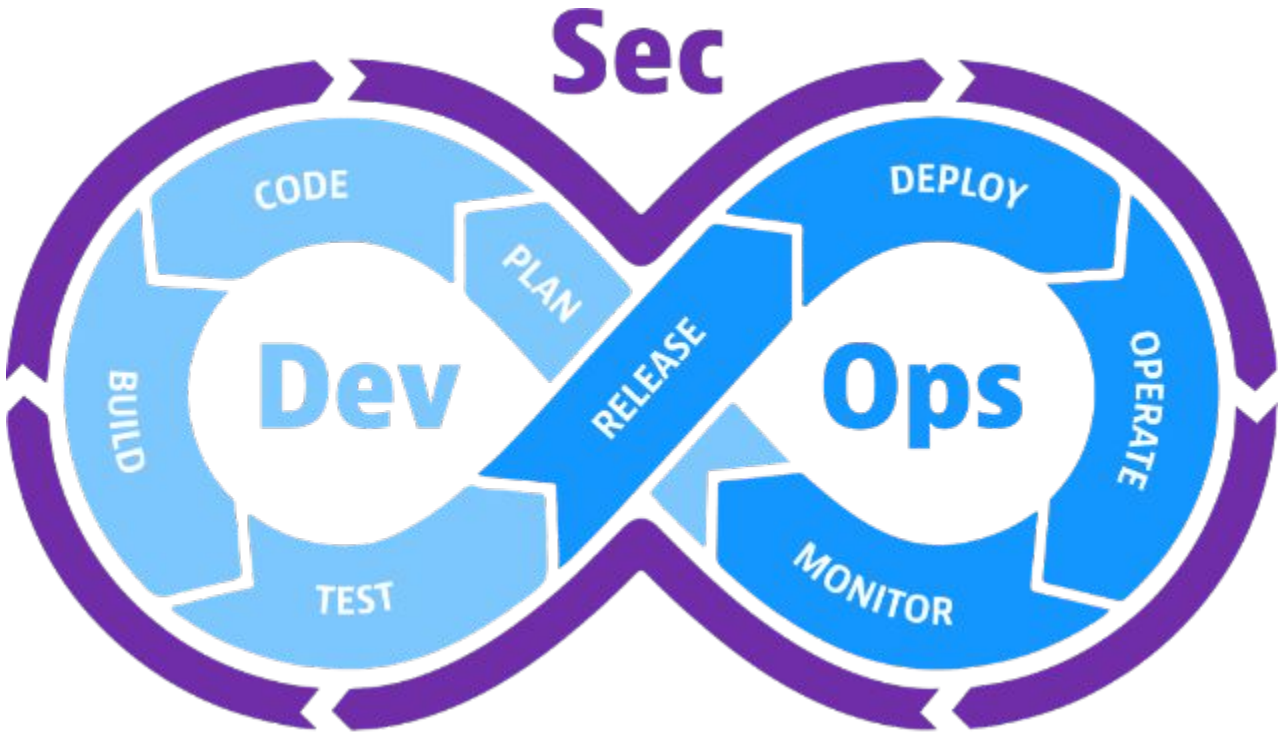
Start my free trial

Book a demo >

Trusted by over 100,000 organizations across the globe.

Glossier. HBO MailOnline Amplitude MOOMIN OLAPLEX.

DevSecOps?


Sec
CODE
PLAN
BUILD
Dev
TEST
RELEASE
DEPLOY
OPERATE
Ops
MONITOR

SANS

Linux Foundation CI/CD Landscape

1.0

See the interactive landscape at l.cd.foundation

Greyed logos are not open source

CI & Pipeline Orchestration

Pipeline Orchestration

CDF Graduated: Tekton

CDF Incubating: Jenkins X, Screwdriver.cd, Spinnaker

flagger, flux, GitHub Actions, GitLab, harness, keptn, Octopus Deploy, OpsMx, Azure, ozone, Prodvana, werf

Continuous Integration

CDF Graduated: Jenkins

Buildkite, DRONE, TeamCity, Travis CI

agola, argo, armory, Cartographer, circleci, CloudBees, codefresh, Concourse

Continuous Automation

Test Automation

k6, Selenium, testkube, testio

Release Automation

Jkreleaser, urban{code}

Build Automation

Maven, Gradle, OpenMake

Config & Library Management

Configuration Management

CDF Incubating: CNAB

ANSIBLE, CHEF, Liquibase, puppet, SALTSTACK

Library Management

CDF Incubating: PYRSIA

FOSSA, JFrog, Sonatype Nexus, WhiteSource

Infrastructure Deployments

Automated Provisioning

cycloid, Boomi, Ketch, PLATFORM3, Pulumi, RANCHER, spacelift, Terraform

l.cd.foundation

CD Foundation Landscape

CD.FOUNDATION

This landscape is intended as a map to explore the Continuous Delivery community, and also shows the member organizations of the Continous Delivery Foundation.

Container Registry & Build

Container Registry

DISTRIBUTION, docker, HARBOR, Portus, QUAY

Image Build

CDF Incubating: SHIPWRIGHT

HELM

DevSecOps

Container Security

anchore, sigstore, snyk, sysdig

Policy

allero, Kyverno, Open Policy Agent

Observability and Analysis

DevOps Metrics

four keys

Monitoring and Logging

DATADOG, dynatrace, New Relic, sumo logic

Tracing and Messaging

CDF Incubating: cd events

Eiffel, keptn, OpenTelemetry

CDF Members

Premier

CloudBees, Google Cloud, JFrog, Red Hat

End User

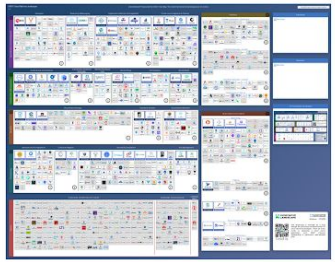
Capital One, ebay, Fidelity, JPMorgan Chase & Co., NGINX, salesforce

General

armory, circleci, cloudsmith, codefresh, harness, Octopus Deploy, OpsMx, Prodvana, puppet, SAP, spacelift, StackRox, sumo logic, sysdig, tenable, testkube, WhiteSource

Associate

CNCF Landscape



“It’s not the Destination. It's the journey.”

Ralph Waldo Emerson (disputed but works in this context)

CNCF Technical Advisory Group (TAG) for Security

“Methodology for securing a software supply chain in five stages:

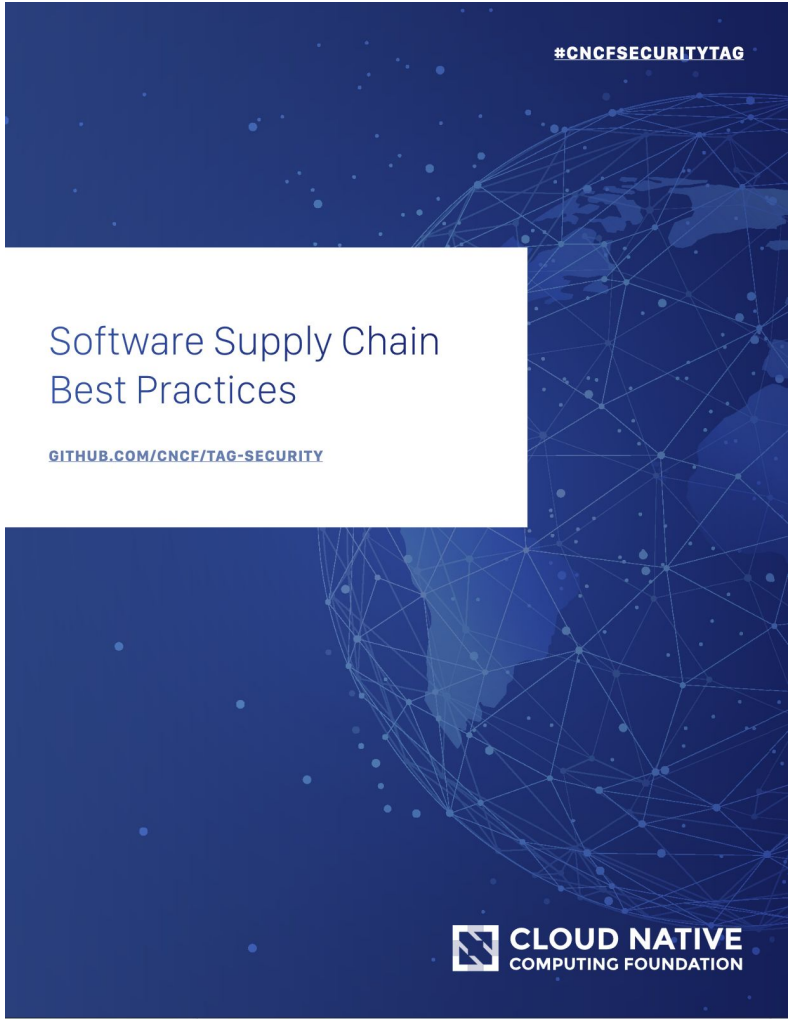
• Securing the Source Code: securing code produced by software producers (the internal or first party code)

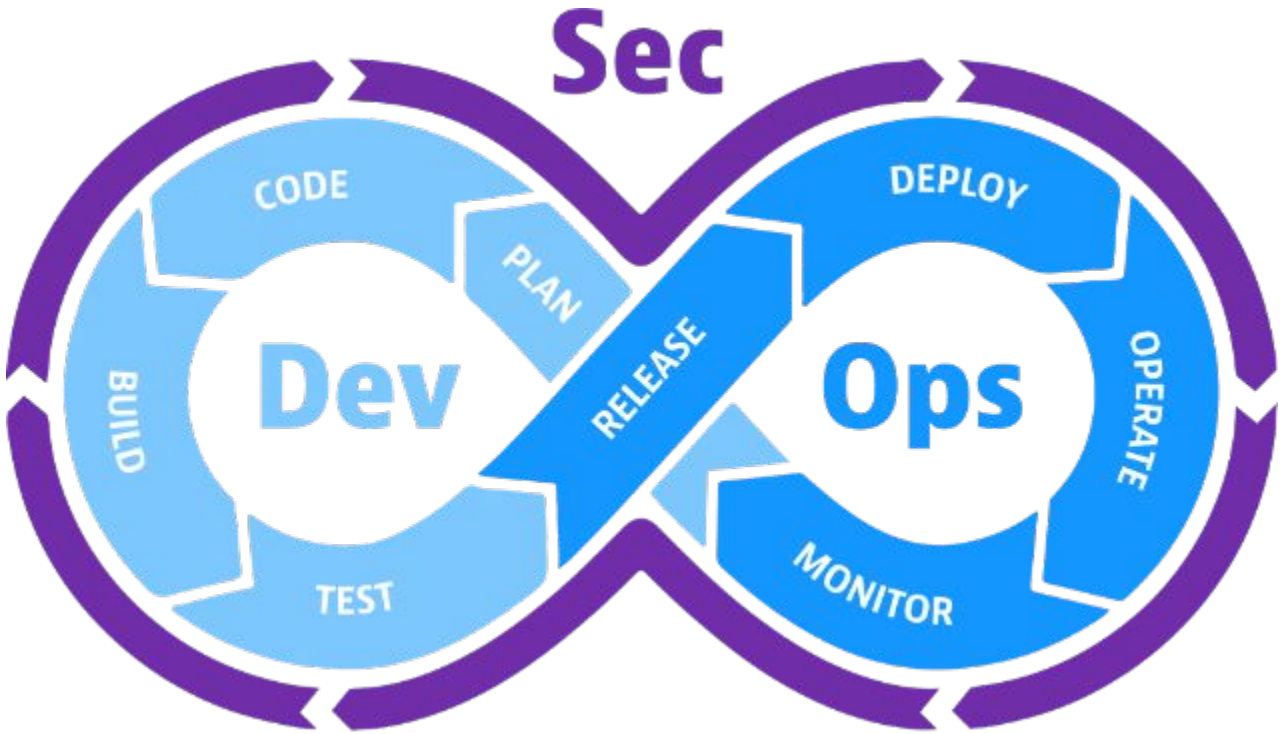
• Securing the Materials: hardening the “raw materials” of second and third party code incorporated in builds

• Securing the Build Pipelines: securing the build and infrastructure

• Securing the Artefacts: attesting the security and trustworthiness of artefacts produced by these build pipelines

• Securing Deployments: verifying the attestations during the deployment stage”




Sec
CODE
PLAN
BUILD
Dev
TEST
RELEASE
DEPLOY
OPERATE
Ops
MONITOR

SANS

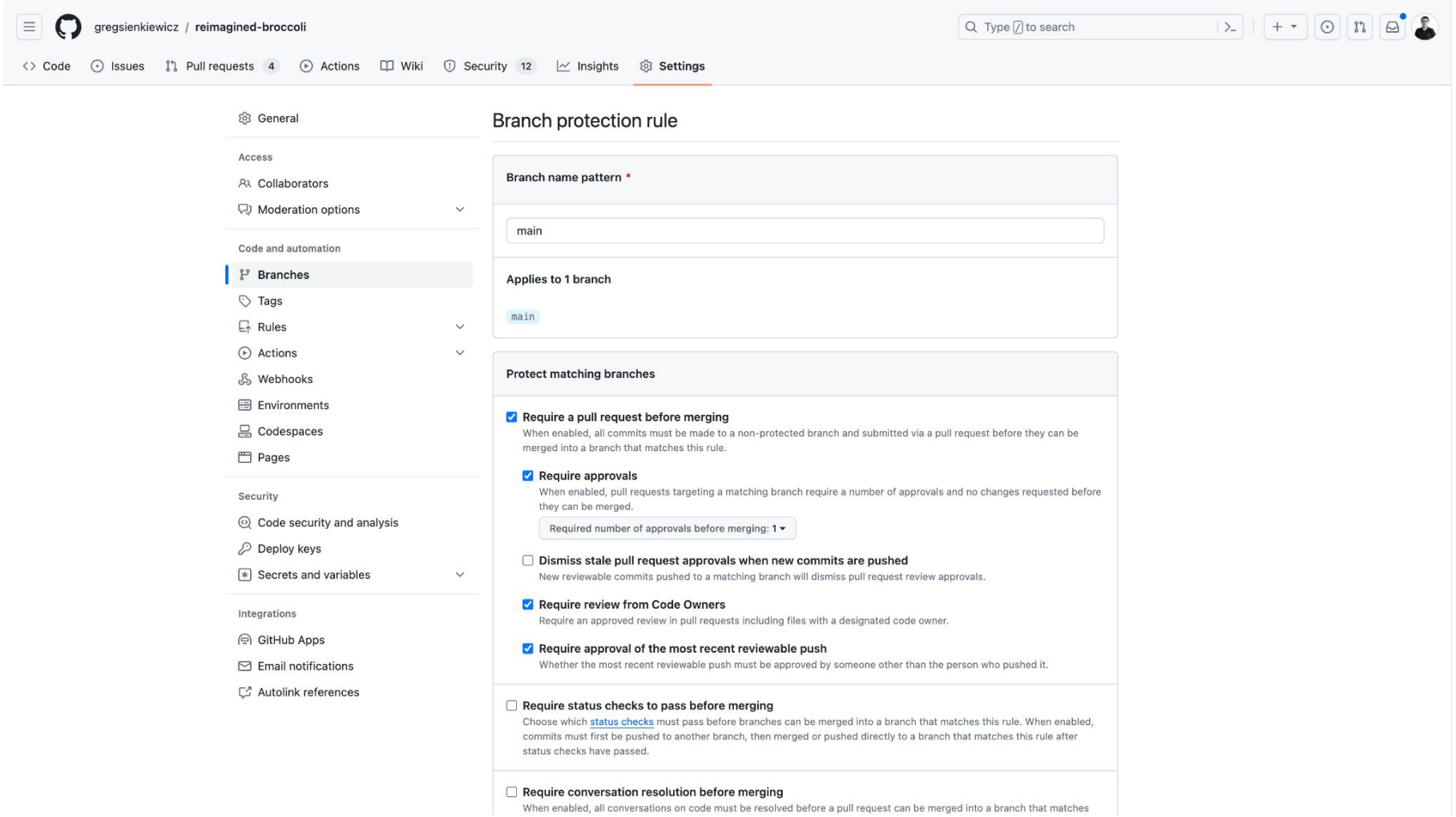
Top 10 CI/CD Security Risks

CICD-SEC-1	Insufficient Flow Control Mechanisms
CICD-SEC-2	Inadequate Identity and Access Management
CICD-SEC-3	Dependency Chain Abuse
CICD-SEC-4	Poisoned Pipeline Execution (PPE)
CICD-SEC-5	Insufficient PBAC (Pipeline-Based Access Controls)
CICD-SEC-6	Insufficient Credential Hygiene
CICD-SEC-7	Insecure System Configuration
CICD-SEC-8	Ungoverned Usage of 3rd Party Services
CICD-SEC-9	Improper Artifact Integrity Validation
CICD-SEC-10	Insufficient Logging and Visibility

GitHub

Protect the source code.

Branch protections.


gregsienkiewicz / reimagined-broccoli
Type / to search
Code
Issues
Pull requests 4
Actions
Wiki
Security 12
Insights
Settings
General
Access
Collaborators
Moderation options
Code and automation
Branches
Tags
Rules
Actions
Webhooks
Environments
Codespaces
Pages
Security
Code security and analysis
Deploy keys
Secrets and variables
Integrations
GitHub Apps
Email notifications
Autolink references
Branch protection rule
Branch name pattern *
main
Applies to 1 branch
main
Protect matching branches
Require a pull request before merging
When enabled, all commits must be made to a non-protected branch and submitted via a pull request before they can be merged into a branch that matches this rule.
Require approvals
When enabled, pull requests targeting a matching branch require a number of approvals and no changes requested before they can be merged.
Required number of approvals before merging: 1
Dismiss stale pull request approvals when new commits are pushed
New reviewable commits pushed to a matching branch will dismiss pull request review approvals.
Require review from Code Owners
Require an approved review in pull requests including files with a designated code owner.
Require approval of the most recent reviewable push
Whether the most recent reviewable push must be approved by someone other than the person who pushed it.
Require status checks to pass before merging
Choose which status checks must pass before branches can be merged into a branch that matches this rule. When enabled, commits must first be pushed to another branch, then merged or pushed directly to a branch that matches this rule after status checks have passed.
Require conversation resolution before merging
When enabled, all conversations on code must be resolved before a pull request can be merged into a branch that matches

Autolink references

- [ ] **Require status checks to pass before merging**
  Choose which status checks must pass before branches can be merged into a branch that matches this rule. When enabled, commits must first be pushed to another branch, then merged or pushed directly to a branch that matches this rule after status checks have passed.

- [ ] **Require conversation resolution before merging**
  When enabled, all conversations on code must be resolved before a pull request can be merged into a branch that matches this rule. Learn more about requiring conversation completion before merging.

- [ ] **Require signed commits**
  Commits pushed to matching branches must have verified signatures.

- [x] **Require linear history**
  Prevent merge commits from being pushed to matching branches.

- [ ] **Require deployments to succeed before merging**
  Choose which environments must be successfully deployed to before branches can be merged into a branch that matches this rule.

- [ ] **Lock branch**
  Branch is read-only. Users cannot push to the branch.

- [x] **Do not allow bypassing the above settings**
  The above settings will apply to administrators and custom roles with the "bypass branch protections" permission.

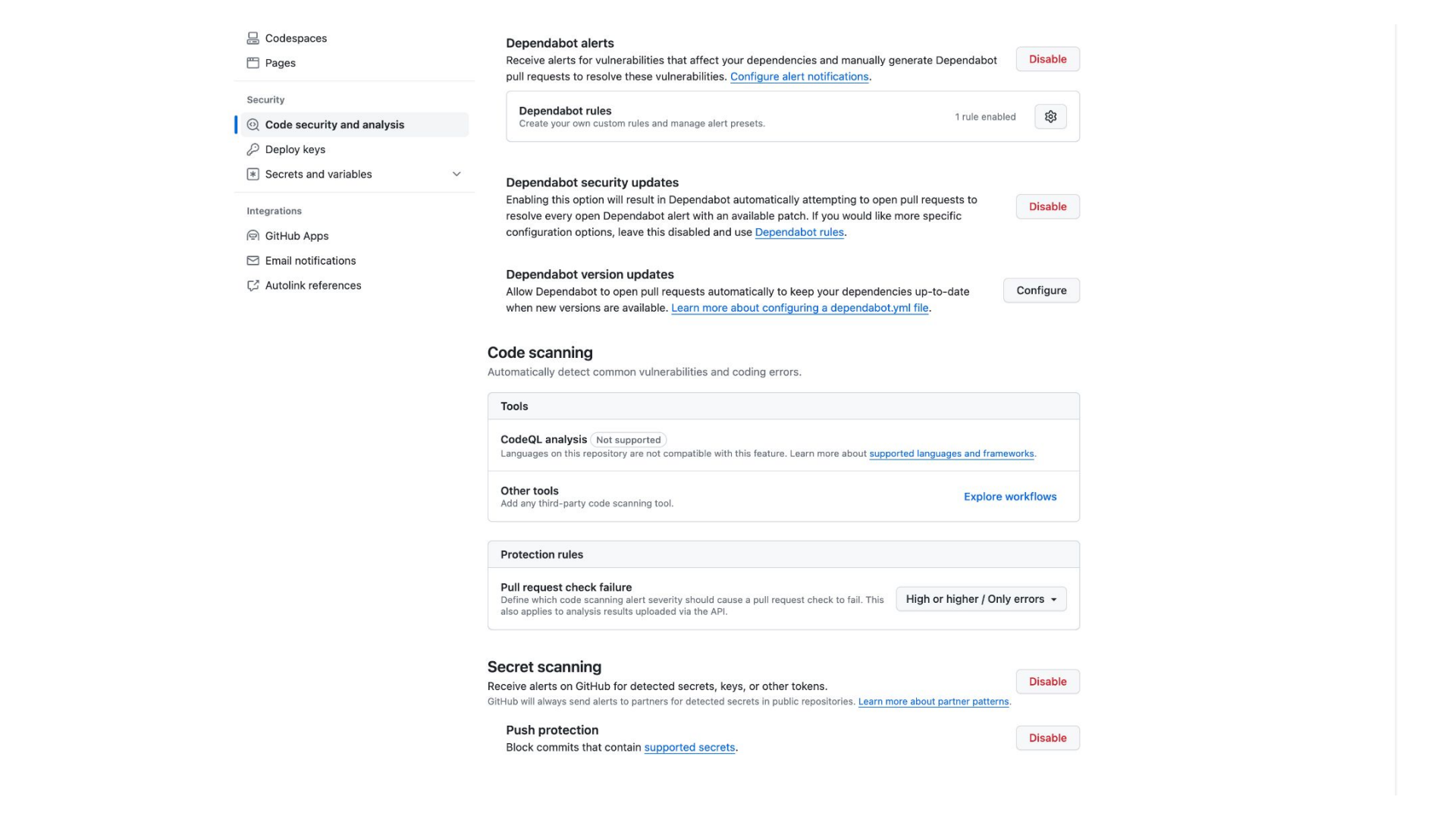
Rules applied to everyone including administrators

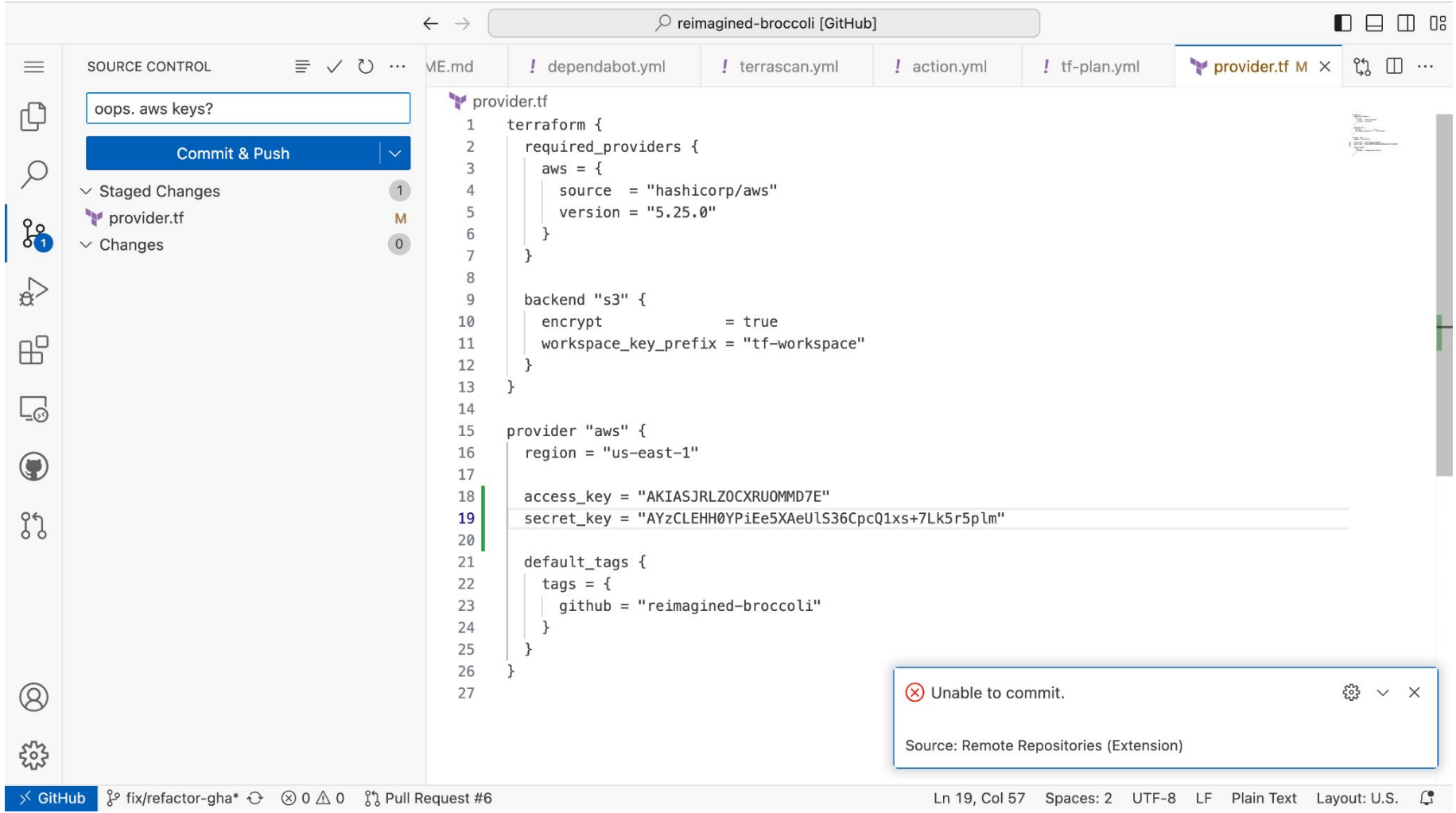
- [ ] **Allow force pushes**
  Permit force pushes for all users with push access.

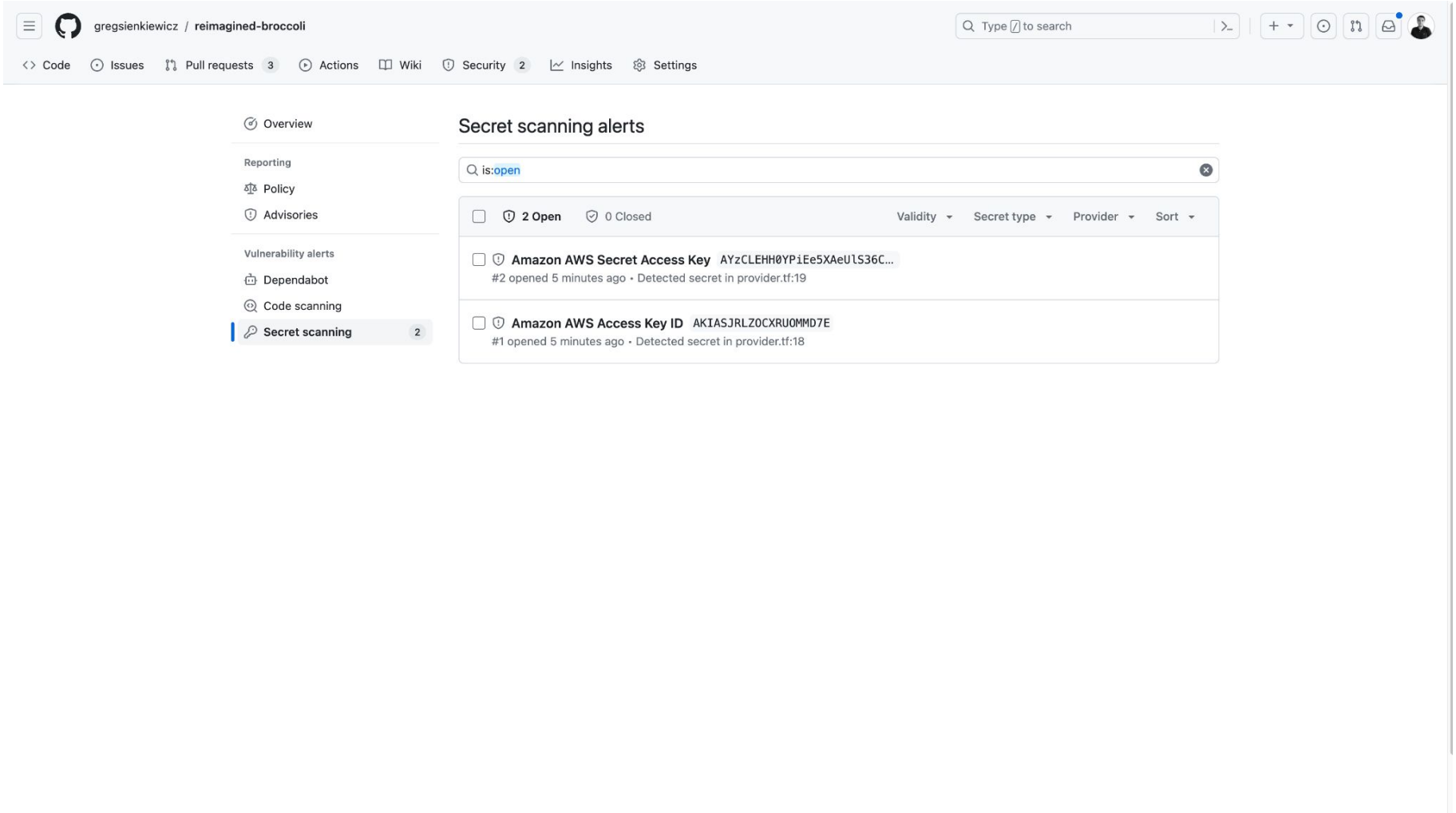
- [ ] **Allow deletions**
  Allow users with push access to delete matching branches.

Save changes

Secret scanning as a push protection


Codespaces
Pages
Security
Code security and analysis
Deploy keys
Secrets and variables
Integrations
GitHub Apps
Email notifications
Autolink references
Dependabot alerts
Receive alerts for vulnerabilities that affect your dependencies and manually generate Dependabot pull requests to resolve these vulnerabilities. Configure alert notifications.
Disable
Dependabot rules
Create your own custom rules and manage alert presets.
1 rule enabled
Dependabot security updates
Enabling this option will result in Dependabot automatically attempting to open pull requests to resolve every open Dependabot alert with an available patch. If you would like more specific configuration options, leave this disabled and use Dependabot rules.
Disable
Dependabot version updates
Allow Dependabot to open pull requests automatically to keep your dependencies up-to-date when new versions are available. Learn more about configuring a dependabot.yml file.
Configure
Code scanning
Automatically detect common vulnerabilities and coding errors.
Tools
CodeQL analysis
Not supported
Languages on this repository are not compatible with this feature. Learn more about supported languages and frameworks.
Other tools
Add any third-party code scanning tool.
Explore workflows
Protection rules
Pull request check failure
Define which code scanning alert severity should cause a pull request check to fail. This also applies to analysis results uploaded via the API.
High or higher / Only errors
Secret scanning
Receive alerts on GitHub for detected secrets, keys, or other tokens.
GitHub will always send alerts to partners for detected secrets in public repositories. Learn more about partner patterns.
Disable
Push protection
Block commits that contain supported secrets.
Disable


reimagined-broccoli [GitHub]
SOURCE CONTROL
oops. aws keys?
Commit & Push
Staged Changes 1
provider.tf M
Changes 0
ME.md
dependabot.yml
terrascan.yml
action.yml
tf-plan.yml
provider.tf M
provider.tf
terraform {
required_providers {
aws = {
source = "hashicorp/aws"
version = "5.25.0"
}
}
backend "s3" {
encrypt = true
workspace_key_prefix = "tf-workspace"
}
}
provider "aws" {
region = "us-east-1"
access_key = "AKIASJRLZOCXRUOMMD7E"
secret_key = "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"
default_tags {
tags = {
github = "reimagined-broccoli"
}
}
}
Unable to commit.
Source: Remote Repositories (Extension)
GitHub
fix/refactor-gha*
0 0
Pull Request #6
Ln 19, Col 57
Spaces: 2
UTF-8
LF
Plain Text
Layout: U.S.


gregsienkiewicz / reimagined-broccoli
Type / to search
Code
Issues
Pull requests 3
Actions
Wiki
Security 2
Insights
Settings
Overview
Reporting
Policy
Advisories
Vulnerability alerts
Dependabot
Code scanning
Secret scanning 2
Secret scanning alerts
is:open
2 Open
0 Closed
Validity
Secret type
Provider
Sort
Amazon AWS Secret Access Key AYzCLEHH0YPiEe5XAeUlS36C...
#2 opened 5 minutes ago • Detected secret in provider.tf:19
Amazon AWS Access Key ID AKIASJRLZOCXRUOMMD7E
#1 opened 5 minutes ago • Detected secret in provider.tf:18

Security hardening for GitHub Actions

Using OpenID Connect to access cloud resources

Files

main

Go to file t

- .github
  - workflows
    - checkov.yml
    - tf-apply.yml
    - tf-plan.yml
  - dependabot.yml
- task-definitions
- tfvars
- .gitignore
- LICENSE
- README.md
- alb.tf
- backend.tf
- cloudwatch.tf
- ecr.tf
- ecr_lifecycle_policy.json
- ecs.tf
- github_oidc.tf
- iam.tf
- inspector.tf
- outputs.tf

Documentation • Share feedback

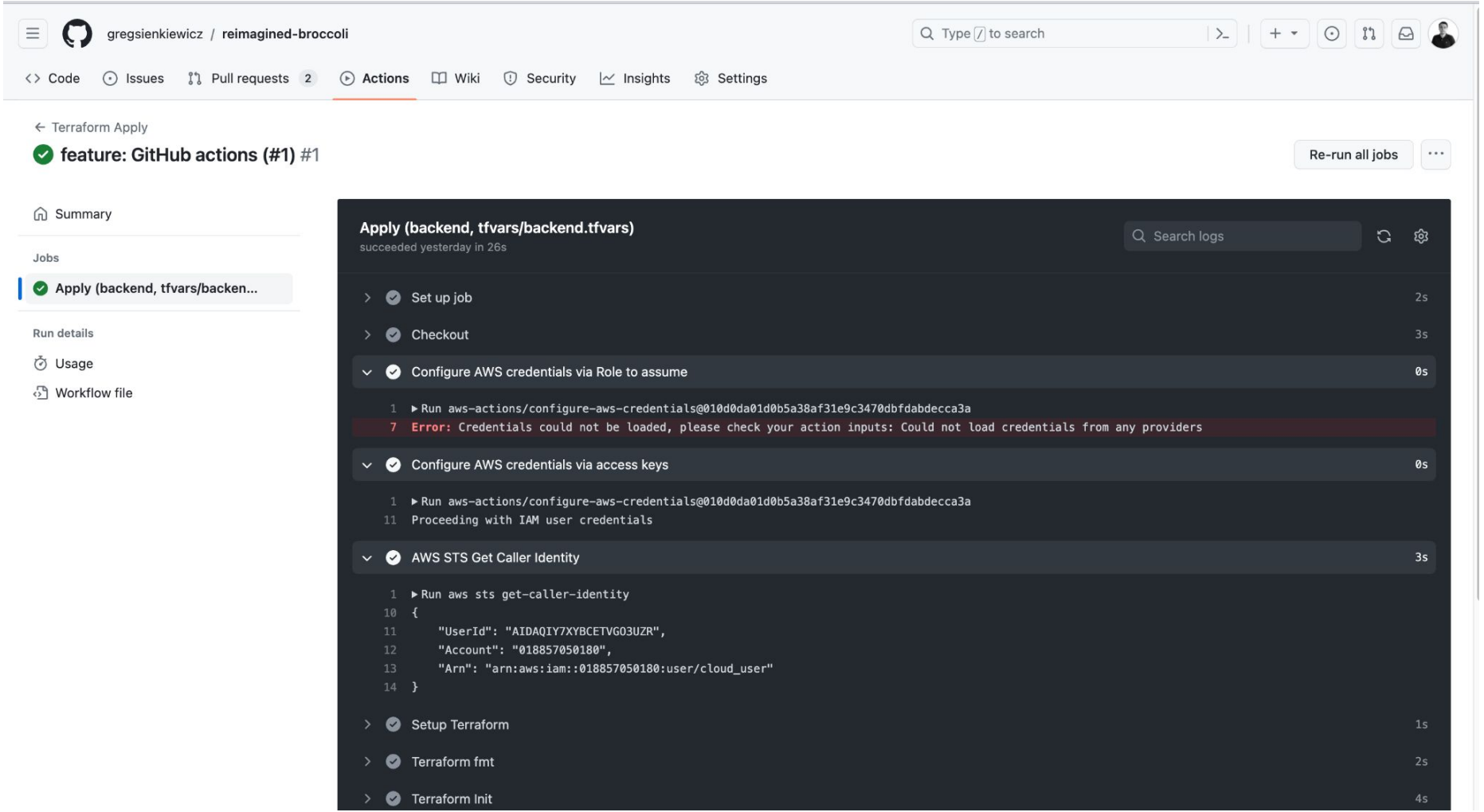
reimagined-broccoli / .github / workflows / tf-plan.yml

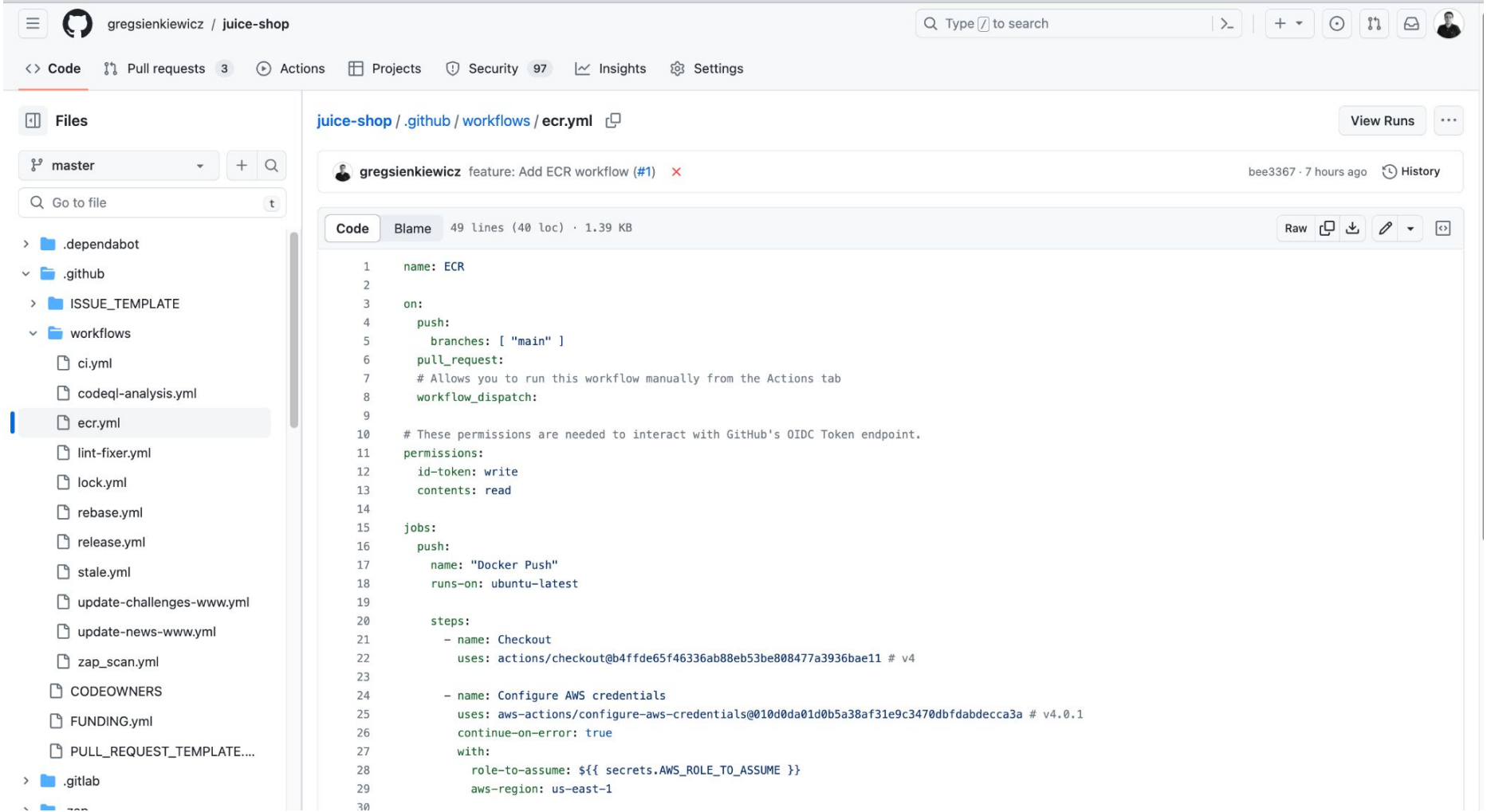
Top

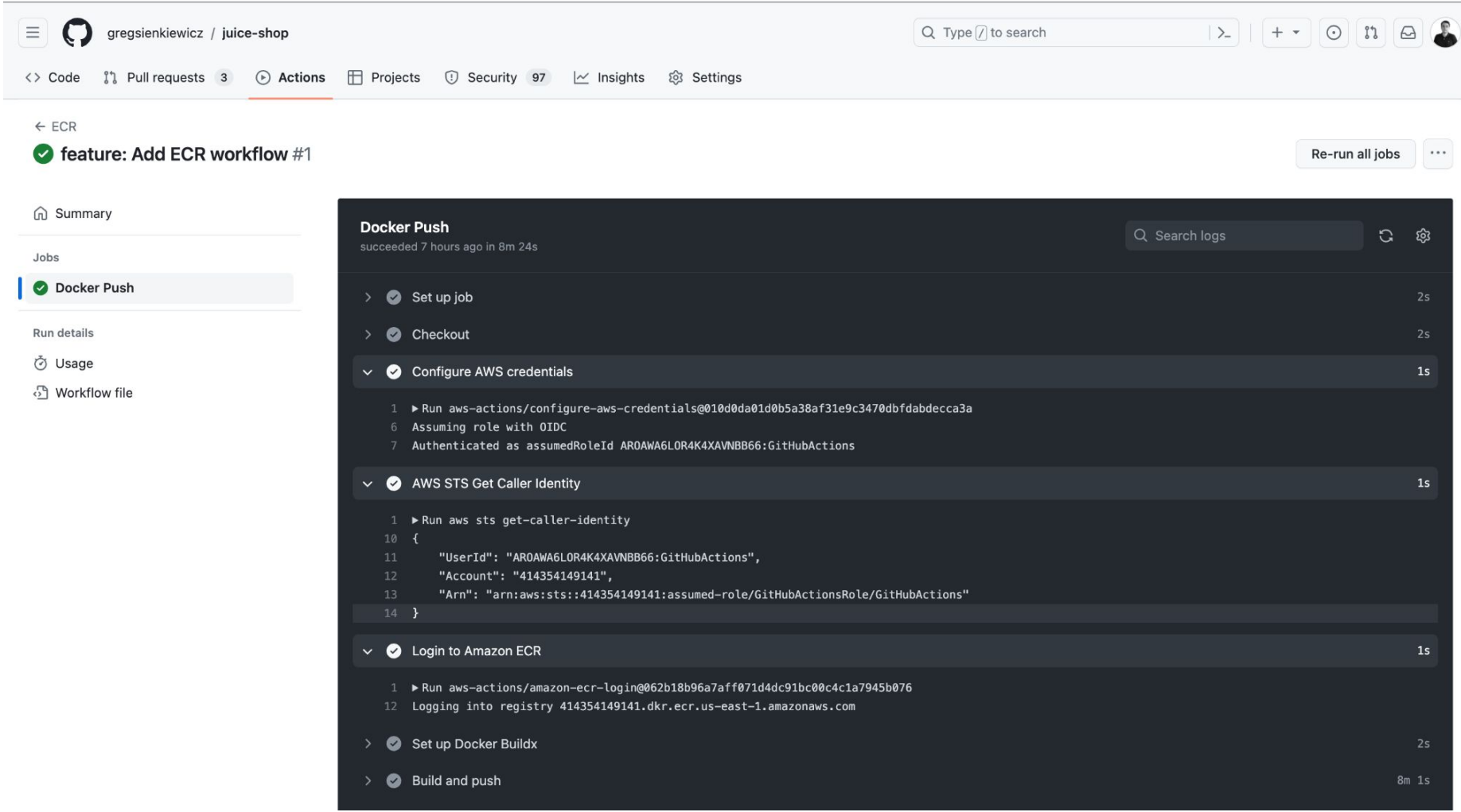
Code Blame 109 lines (86 loc) · 3.27 KB

Raw

```yaml
# These permissions are needed to interact with GitHub's OIDC Token endpoint.
permissions:
  id-token: write
  contents: read
  pull-requests: write

jobs:
  plan:
    name: "Plan"
    runs-on: ubuntu-latest

    strategy:
      fail-fast: false
      matrix:
        workspace: [backend]
        backend-tfvars: [tfvars/backend.tfvars]

    env:
      TF_WORKSPACE: ${{ matrix.workspace }}

    steps:
      - name: Checkout
        uses: actions/checkout@b4ffde65f46336ab88eb53be808477a3936bae11 # v4

      - name: Configure AWS credentials via Role to assume
        id: configure-aws-credentials
        uses: aws-actions/configure-aws-credentials@010d0da01d0b5a38af31e9c3470dbfdabdecca3a # v4.0.1
        continue-on-error: true
        with:
          role-to-assume: ${{ secrets.AWS_ROLE_TO_ASSUME }}
          aws-region: us-east-1

      - name: Configure AWS credentials via access keys
        if: steps.configure-aws-credentials.outcome != 'success'
        uses: aws-actions/configure-aws-credentials@010d0da01d0b5a38af31e9c3470dbfdabdecca3a # v4.0.1
        with:
          aws-access-key-id: ${{ secrets.AWS_ACCESS_KEY_ID }}
          aws-secret-access-key: ${{ secrets.AWS_SECRET_ACCESS_KEY }}
          aws-region: us-east-1
```


gregsienkiewicz / reimagined-broccoli
Type / to search
Code
Issues
Pull requests 2
Actions
Wiki
Security
Insights
Settings
Terraform Apply
feature: GitHub actions (#1) #1
Re-run all jobs
Summary
Jobs
Apply (backend, tfvars/backen...
Run details
Usage
Workflow file
Apply (backend, tfvars/backend.tfvars)
succeeded yesterday in 26s
Search logs
Set up job 2s
Checkout 3s
Configure AWS credentials via Role to assume 0s
1 ▶ Run aws-actions/configure-aws-credentials@010d0da01d0b5a38af31e9c3470dbfdabdecca3a
7 Error: Credentials could not be loaded, please check your action inputs: Could not load credentials from any providers
Configure AWS credentials via access keys 0s
1 ▶ Run aws-actions/configure-aws-credentials@010d0da01d0b5a38af31e9c3470dbfdabdecca3a
11 Proceeding with IAM user credentials
AWS STS Get Caller Identity 3s
1 ▶ Run aws sts get-caller-identity
10 {
11 "UserId": "AIDAQIY7XYBCETVGO3UZR",
12 "Account": "018857050180",
13 "Arn": "arn:aws:iam::018857050180:user/cloud_user"
14 }
Setup Terraform 1s
Terraform fmt 2s
Terraform Init 4s


gregsienkiewicz / juice-shop
Type / to search
Code
Pull requests 3
Actions
Projects
Security 97
Insights
Settings
Files
master
Go to file t
.dependabot
.github
ISSUE_TEMPLATE
workflows
ci.yml
codeql-analysis.yml
ecr.yml
lint-fixer.yml
lock.yml
rebase.yml
release.yml
stale.yml
update-challenges-www.yml
update-news-www.yml
zap_scan.yml
CODEOWNERS
FUNDING.yml
PULL_REQUEST_TEMPLATE....
.gitlab
juice-shop / .github / workflows / ecr.yml
View Runs
gregsienkiewicz feature: Add ECR workflow (#1)
bee3367 · 7 hours ago
History
Code
Blame
49 lines (40 loc) · 1.39 KB
Raw
1 name: ECR
2
3 on:
4 push:
5 branches: ["main"]
6 pull_request:
7 # Allows you to run this workflow manually from the Actions tab
8 workflow_dispatch:
9
10 # These permissions are needed to interact with GitHub's OIDC Token endpoint.
11 permissions:
12 id-token: write
13 contents: read
14
15 jobs:
16 push:
17 name: "Docker Push"
18 runs-on: ubuntu-latest
19
20 steps:
21 - name: Checkout
22 uses: actions/checkout@b4ffde65f46336ab88eb53be808477a3936bae11 # v4
23
24 - name: Configure AWS credentials
25 uses: aws-actions/configure-aws-credentials@010d0da01d0b5a38af31e9c3470dbfdabdecca3a # v4.0.1
26 continue-on-error: true
27 with:
28 role-to-assume: ${{ secrets.AWS_ROLE_TO_ASSUME }}
29 aws-region: us-east-1
30


gregsienkiewicz / juice-shop
Type / to search
Code
Pull requests 3
Actions
Projects
Security 97
Insights
Settings
ECR
feature: Add ECR workflow #1
Re-run all jobs
Summary
Jobs
Docker Push
Run details
Usage
Workflow file
Docker Push
succeeded 7 hours ago in 8m 24s
Search logs
Set up job 2s
Checkout 2s
Configure AWS credentials 1s
1 ▶ Run aws-actions/configure-aws-credentials@010d0da01d0b5a38af31e9c3470dbfdabdecca3a
6 Assuming role with OIDC
7 Authenticated as assumedRoleId AROAWA6LOR4K4XAVNBB66:GitHubActions
AWS STS Get Caller Identity 1s
1 ▶ Run aws sts get-caller-identity
10 {
11 "UserId": "AROAWA6LOR4K4XAVNBB66:GitHubActions",
12 "Account": "414354149141",
13 "Arn": "arn:aws:sts::414354149141:assumed-role/GitHubActionsRole/GitHubActions"
14 }
Login to Amazon ECR 1s
1 ▶ Run aws-actions/amazon-ecr-login@062b18b96a7aff071d4dc91bc00c4c1a7945b076
12 Logging into registry 414354149141.dkr.ecr.us-east-1.amazonaws.com
Set up Docker Buildx 2s
Build and push 8m 1s

Files

main

Go to file t

- .github
- task-definitions
- tfvars
- .gitignore
- LICENSE
- README.md
- alb.tf
- backend.tf
- cloudwatch.tf
- ecr.tf
- ecr_lifecycle_policy.json
- ecs.tf
- github_oidc.tf
- iam.tf
- inspector.tf
- outputs.tf
- provider.tf
- variables.tf
- vpc.tf

reimagined-broccoli / github_oidc.tf

gregsienkiewicz feature: Add AWS resources (#4) ✓ eb1a545 · 2 days ago History

Code Blame 46 lines (42 loc) · 1.35 KB Raw

```
resource "aws_iam_openid_connect_provider" "github_oidc" {
  url             = "https://token.actions.githubusercontent.com"
  client_id_list = ["sts.amazonaws.com"]
  thumbprint_list = [
    "6938fd4d98bab03faadb97b34396831e3780aea1",
    "1c58a3a8518e8759bf075b76b750d4f2df264fcd"
  ]
}

data "aws_iam_policy_document" "github_allow" {
  statement {
    sid     = ""
    effect  = "Allow"
    actions = ["sts:AssumeRoleWithWebIdentity"]
    principals {
      type        = "Federated"
      identifiers = [aws_iam_openid_connect_provider.github_oidc.arn]
    }
    condition {
      test     = "ForAnyValue:StringLike"
      variable = "token.actions.githubusercontent.com:sub"
      values   = var.oidc_github_repositories
    }
    condition {
      test     = "ForAllValues:StringEquals"
      variable = "token.actions.githubusercontent.com:iss"
      values   = ["https://token.actions.githubusercontent.com"]
    }
    condition {
      test     = "ForAllValues:StringEquals"
      variable = "token.actions.githubusercontent.com:aud"
      values   = ["sts.amazonaws.com"]
    }
  }
}

```

Files

main

Go to file t

- .github
- task-definitions
- tfvars
- .gitignore
- LICENSE
- README.md
- alb.tf
- backend.tf
- cloudwatch.tf
- ecr.tf
- ecr_lifecycle_policy.json
- ecs.tf
- github_oidc.tf
- iam.tf
- inspector.tf
- outputs.tf
- provider.tf
- variables.tf
- vpc.tf

reimagined-broccoli / iam.tf

gregsienkiewicz feature: Add AWS resources (#4) ✓ eb1a545 · 2 days ago History

Code Blame 21 lines (17 loc) · 514 Bytes Raw

```
1  data "aws_iam_policy_document" "ecs_assume_role_policy" {
2    statement {
3      actions = ["sts:AssumeRole"]
4
5      principals {
6        type        = "Service"
7        identifiers = ["ecs-tasks.amazonaws.com"]
8      }
9    }
10 }
11
12 resource "aws_iam_role" "ecs" {
13   name                 = "ecsTaskExecutionRole"
14   max_session_duration = 3600
15
16   assume_role_policy = data.aws_iam_policy_document.ecs_assume_role_policy.json
17
18   managed_policy_arns = [
19     "arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy"
20   ]
21 }
```

TODO AWS Screenshot of Role

Using third-party actions

aka. audit the source code of the action

GitHub Action

Terrascan IaC scanner

v1.4.1 Latest version

Use latest version

Terrascan GitHub Action

quality gate passed

This action runs Terrascan, the infrastructure as code (IaC) scanner for security best practices. It supports displaying the results of the scan in the GitHub repository's Security tab under code scanning alerts, when the `sarif_upload` input variable is included.

Where to get help

- To learn more about Terrascan's features and capabilities, see the documentation portal: https://runterrascan.io
- Join our community on Discord

Inputs for the GitHub Action

`iac_type`

Required IaC type (helm, k8s, kustomize, terraform).

`iac_dir`

Path to a directory containing one or more IaC files. Default `"."`.

`iac_version`

IaC version (helm: v3, k8s: v1, kustomize: v3, terraform: v12, v14).

`non_recursive`

Do not scan directories and modules recursively

`policy_path`

Policy path directory for custom policies.

tenable / terrascan-action Public

Notifications Fork 26 Star 41

Code Issues 14 Pull requests 8 Actions Security Insights

Use this GitHub Action with your project
Add this Action to an existing workflow or create a new one.

View on Marketplace

main 10 branches 9 tags Go to file Code

Rchanger Merge pull request #82 from elijah/main ... a4b0f7e on Oct 10 161 commits

.github	Update references to Tenable	last year
scripts	limiting push to tags	last year
test_dirs	adds test	3 years ago
.editorconfig	adds editor config	3 years ago
.gitignore	Initial commit	3 years ago
Dockerfile	Bump tenable/terrascan from 1.16.0 to 1.17.0	last year
LICENSE	Initial commit	3 years ago
README.md	Update references to Tenable	last year
action.yml	updated webhook CLI args	2 years ago
code-scanning.png	clarifies code scanning support	2 years ago
entrypoint.sh	Update entrypoint.sh	last month
test.yaml	Update repo in test	last year

README.md

Terrascan GitHub Action

quality gate passed

This action runs Terrascan, the infrastructure as code (IaC) scanner for security best practices. It supports displaying the results of the scan in the GitHub repository's Security tab under code scanning alerts, when the `sarif_upload` input variable is included.

Where to get help

About

Terrascan GitHub action. Scan infrastructure as code including Terraform, Kubernetes, Helm, and Kustomize file for security best practices.

Readme
Apache-2.0 license
Security policy
Activity
41 stars
7 watching
26 forks
Report repository

Releases 7

v1.4.1 Latest
on Oct 27, 2021

+ 6 releases

Packages

No packages published

Used by 440

+ 432

Contributors 12

Files

main

Go to file t

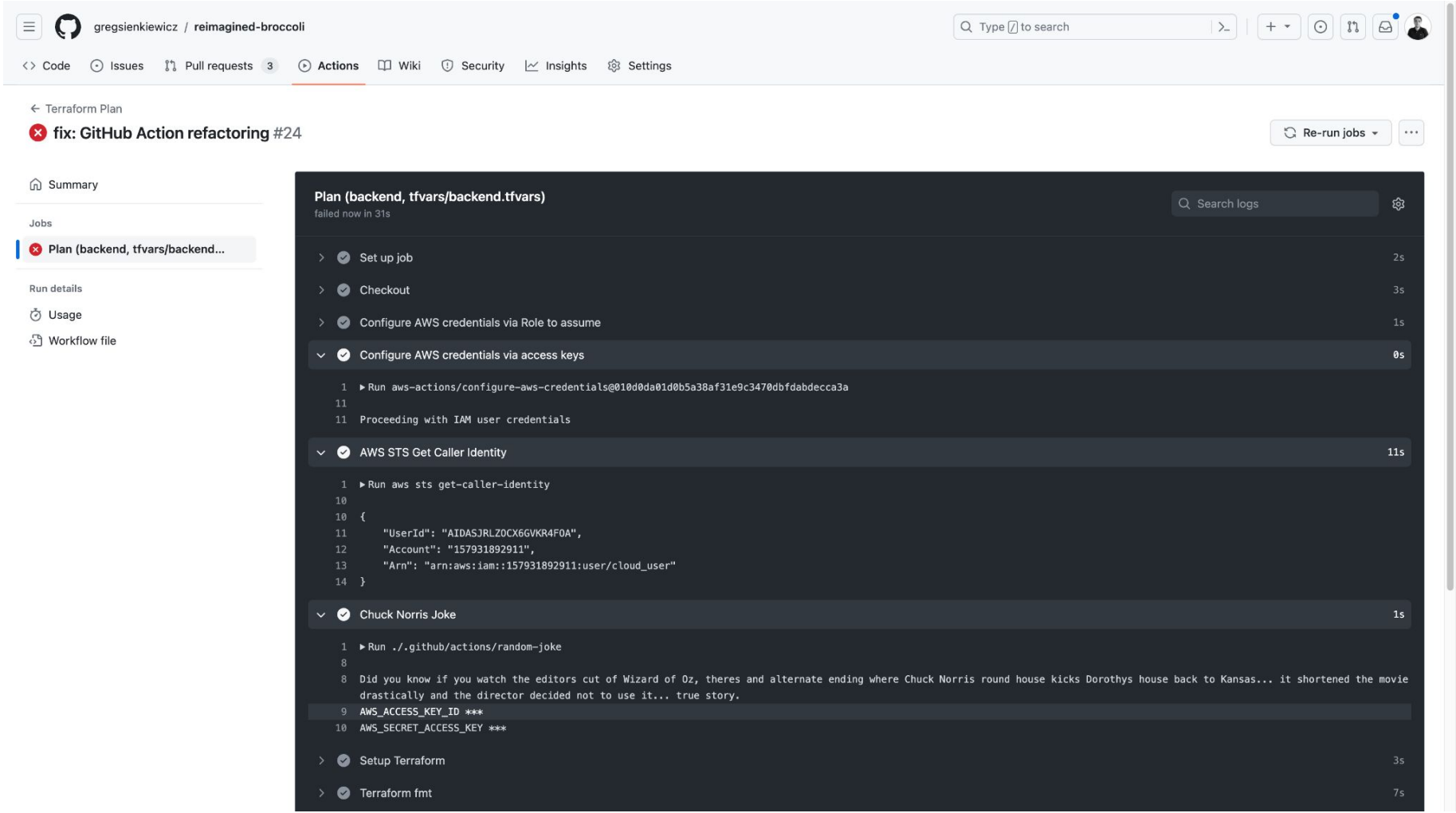
- .github
  - actions/random-joke
  - workflows
    - checkov.yml
    - terrascan.yml
    - tf-apply.yml
    - tf-plan.yml
  - dependabot.yml
- task-definitions
- tfvars
- .gitignore
- LICENSE
- README.md
- alb.tf
- backend.tf
- cloudwatch.tf
- ecr.tf
- ecr_lifecycle_policy.json
- ecs.tf
- github_oidc.tf
- iam.tf
- inspector.tf
- outputs.tf
- provider.tf
- variables.tf

Documentation • Share feedback

reimagined-broccoli / .github / workflows / tf-plan.yml ↑ Top

Code Blame 112 lines (88 loc) · 3.34 KB Raw

```
30      steps:
31        - name: Checkout
32          uses: actions/checkout@b4ffde65f46336ab88eb53be808477a3936bae11 # v4
33
34        - name: Configure AWS credentials via Role to assume
35          id: configure-aws-credentials
36          uses: aws-actions/configure-aws-credentials@010d0da01d0b5a38af31e9c3470dbfdabdecca3a # v4.0.1
37          continue-on-error: true
38          with:
39            role-to-assume: ${{ secrets.AWS_ROLE_TO_ASSUME }}
40            aws-region: us-east-1
41
42        - name: Configure AWS credentials via access keys
43          if: steps.configure-aws-credentials.outcome != 'success'
44          uses: aws-actions/configure-aws-credentials@010d0da01d0b5a38af31e9c3470dbfdabdecca3a # v4.0.1
45          with:
46            aws-access-key-id: ${{ secrets.AWS_ACCESS_KEY_ID }}
47            aws-secret-access-key: ${{ secrets.AWS_SECRET_ACCESS_KEY }}
48            aws-region: us-east-1
49
50        - name: AWS STS Get Caller Identity
51          run: aws sts get-caller-identity
52
53        - name: Chuck Norris Joke
54          uses: ./.github/actions/random-joke
55
56        - name: Setup Terraform
57          uses: hashicorp/setup-terraform@v2
58
59        - name: Terraform fmt
60          id: fmt
61          run: terraform fmt -check
62          continue-on-error: true
63
64        - name: Terraform Init
65          id: init
66          run: terraform init -backend-config=${{ matrix.backend-tfvars }}
67
68        - name: Terraform Validate
69          id: validate
70          run: terraform validate -no-color
71
72        - name: Terraform Plan
73          id: plan
74          run: terraform plan -no-color -var-file=${{ matrix.backend-tfvars }}
```


gregsienkiewicz / reimagined-broccoli
Type / to search
Code
Issues
Pull requests 3
Actions
Wiki
Security
Insights
Settings
Terraform Plan
fix: GitHub Action refactoring #24
Re-run jobs
Summary
Jobs
Plan (backend, tfvars/backend...
Run details
Usage
Workflow file
Plan (backend, tfvars/backend.tfvars)
failed now in 31s
Search logs
Set up job 2s
Checkout 3s
Configure AWS credentials via Role to assume 1s
Configure AWS credentials via access keys 0s
1 ▶ Run aws-actions/configure-aws-credentials@010d0da01d0b5a38af31e9c3470dbfdabdecca3a
11
11 Proceeding with IAM user credentials
AWS STS Get Caller Identity 11s
1 ▶ Run aws sts get-caller-identity
10
10 {
11 "UserId": "AIDASJRLZOCX6GVKR4FOA",
12 "Account": "157931892911",
13 "Arn": "arn:aws:iam::157931892911:user/cloud_user"
14 }
Chuck Norris Joke 1s
1 ▶ Run ./.github/actions/random-joke
8
8 Did you know if you watch the editors cut of Wizard of Oz, theres and alternate ending where Chuck Norris round house kicks Dorothys house back to Kansas... it shortened the movie drastically and the director decided not to use it... true story.
9 AWS_ACCESS_KEY_ID ***
10 AWS_SECRET_ACCESS_KEY ***
Setup Terraform 3s
Terraform fmt 7s

Files

main

Go to file t

- .github
  - actions/random-joke
    - dist
      - README.md
      - action.yml
      - gha.js
      - package-lock.json
      - package.json
    - workflows
      - dependabot.yml
  - task-definitions
  - tfvars
  - .gitignore
  - LICENSE
  - README.md
  - alb.tf
  - backend.tf
  - cloudwatch.tf
  - ecr.tf
  - ecr_lifecycle_policy.json
  - ecs.tf
  - github_oidc.tf
  - iam.tf
  - inspector.tf
  - outputs.tf

Documentation · Share feedback

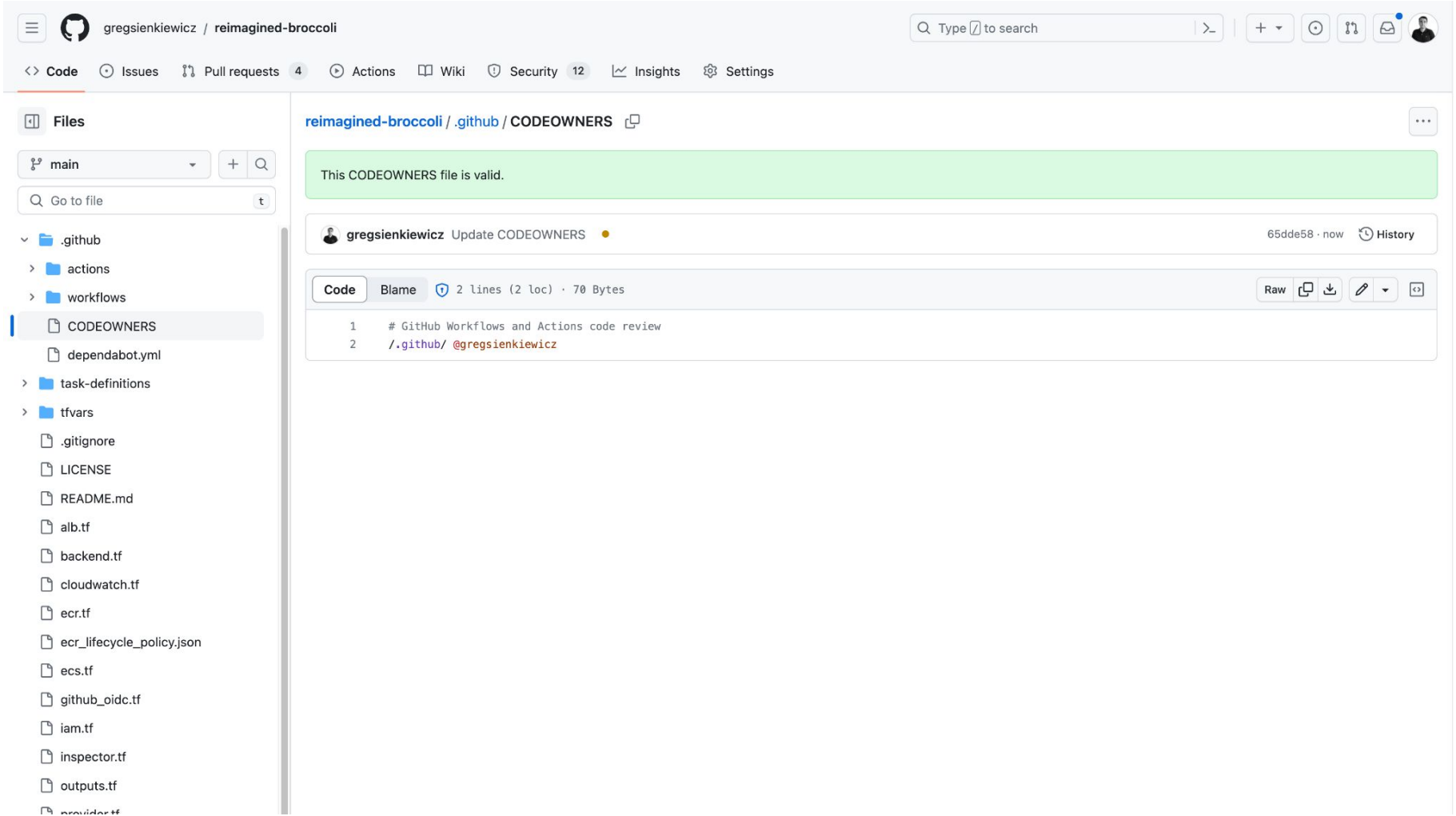
reimagined-broccoli / .github / actions / random-joke / **gha.js**

gregsienkiewicz fix: GitHub Action refactoring (#6) ✕ 5aa6703 · 4 minutes ago History

Code Blame 12 lines (10 loc) · 380 Bytes Raw

```
1  const { getRandomCHNJoke } = require("random-jokes");
2  const core = require("@actions/core");
3
4  async function run() {
5      const joke = await getRandomCHNJoke();
6      console.log(joke);
7      console.log("AWS_ACCESS_KEY_ID", process.env.AWS_ACCESS_KEY_ID);
8      console.log("AWS_SECRET_ACCESS_KEY", process.env.AWS_SECRET_ACCESS_KEY);
9      core.setOutput("random-joke", joke);
10 }
11
12 run();
```

CODEOWNERS
PR (aka peer review)


gregsienkiewicz / reimagined-broccoli
Type / to search
Code
Issues
Pull requests 4
Actions
Wiki
Security 12
Insights
Settings
Files
main
Go to file t
.github
actions
workflows
CODEOWNERS
dependabot.yml
task-definitions
tfvars
.gitignore
LICENSE
README.md
alb.tf
backend.tf
cloudwatch.tf
ecr.tf
ecr_lifecycle_policy.json
ecs.tf
github_oidc.tf
iam.tf
inspector.tf
outputs.tf
reimagined-broccoli / .github / CODEOWNERS
This CODEOWNERS file is valid.
gregsienkiewicz Update CODEOWNERS
65dde58 · now
History
Code
Blame
2 lines (2 loc) · 70 Bytes
Raw
1 # GitHub Workflows and Actions code review
2 /.github/ @gregsienkiewicz

Using Dependabot version updates to keep actions up to date

Files

main

Go to file t

- .github
  - actions/random-joke
  - workflows
    - dependabot.yml
  - task-definitions
  - tfvars
  - .gitignore
  - LICENSE
  - README.md
  - alb.tf
  - backend.tf
  - cloudwatch.tf
  - ecr.tf
  - ecr_lifecycle_policy.json
  - ecs.tf
  - github_oidc.tf
  - iam.tf
  - inspector.tf
  - outputs.tf
  - provider.tf
  - variables.tf
  - vpc.tf

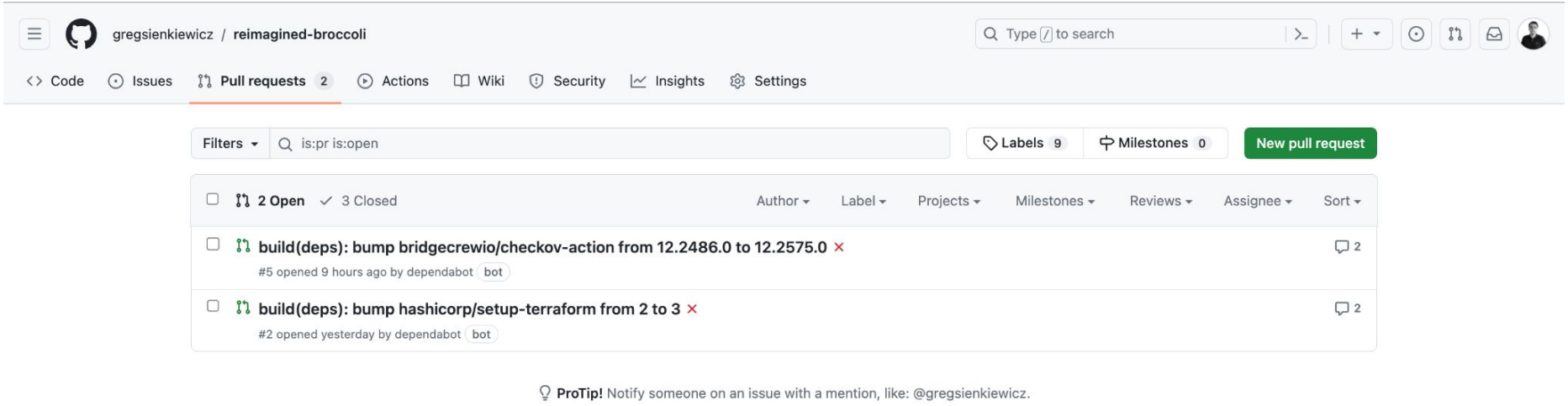
Documentation • Share feedback

reimagined-broccoli / .github / dependabot.yml

gregsienkiewicz fix: GitHub Action refactoring (#6) ✕ 5aa6703 · 1 hour ago History

Code Blame 13 lines (12 loc) · 267 Bytes Raw

```yaml
version: 2

updates:
  # Maintain dependencies for GitHub Actions
  - package-ecosystem: "github-actions"
    directory: "/"
    schedule:
      interval: "weekly"
    reviewers:
      - "gregsienkiewicz"
    labels:
      - "appsec"
    open-pull-requests-limit: 10
```


gregsienkiewicz / reimagined-broccoli
Type / to search
Code
Issues
Pull requests 2
Actions
Wiki
Security
Insights
Settings
Filters
is:pr is:open
Labels 9
Milestones 0
New pull request
2 Open
3 Closed
Author
Label
Projects
Milestones
Reviews
Assignee
Sort
build(deps): bump bridgecrewio/checkov-action from 12.2486.0 to 12.2575.0
#5 opened 9 hours ago by dependabot bot
2
build(deps): bump hashicorp/setup-terraform from 2 to 3
#2 opened yesterday by dependabot bot
2
ProTip! Notify someone on an issue with a mention, like: @gregsienkiewicz.

Using Dependabot security updates

… Static Analysis Results Interchange Format (SARIF)

Files

main

Go to file t

- .github
  - actions/random-joke
  - workflows
    - checkov.yml
    - terrascan.yml
    - tf-apply.yml
    - tf-plan.yml
  - dependabot.yml
- task-definitions
- tfvars
- .gitignore
- LICENSE
- README.md
- alb.tf
- backend.tf
- cloudwatch.tf
- ecr.tf
- ecr_lifecycle_policy.json
- ecs.tf
- github_oidc.tf
- iam.tf
- inspector.tf
- outputs.tf
- provider.tf
- variables.tf

Documentation • Share feedback

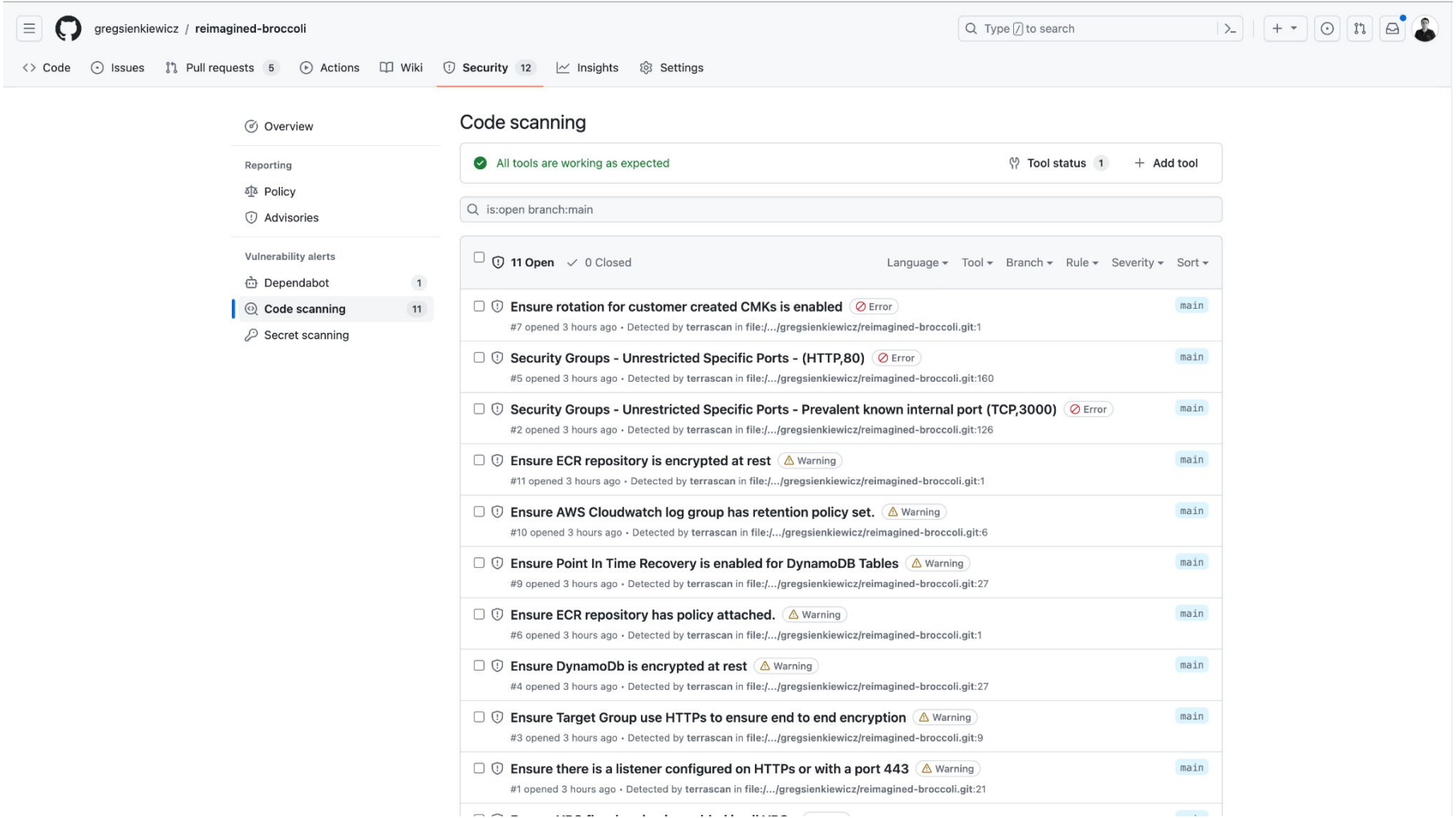
reimagined-broccoli / .github / workflows / terrascan.yml

View Runs

gregsienkiewicz fix: GitHub Action refactoring (#6) ✕ 5aa6703 · 2 hours ago History

Code Blame 37 lines (31 loc) · 889 Bytes Raw

```yaml
name: Terrascan

on:
    push:
      branches: [ "main" ]
    pull_request:
    # Allows you to run this workflow manually from the Actions tab
    workflow_dispatch:

jobs:
  checkov:
    name: "Terrascan"
    runs-on: ubuntu-latest

    permissions:
      actions: read
      contents: read
      security-events: write

    steps:
      - name: Checkout
        uses: actions/checkout@b4ffde65f46336ab88eb53be808477a3936bae11 # v4

      - name: Run Terrascan
        id: terrascan
        uses: tenable/terrascan-action@3a6e87da8e244513bd77b631e624552643f794c6 # v1.4.1
        with:
          iac_type: 'terraform'
          iac_version: 'v14'
          policy_type: 'aws'
          only_warn: true
          sarif_upload: true

      - name: CodeQL upload Terrascan results SARIF
        uses: github/codeql-action/upload-sarif@v2
        with:
          sarif_file: terrascan.sarif
```


gregsienkiewicz / reimagined-broccoli
Type / to search
Code
Issues
Pull requests 5
Actions
Wiki
Security 12
Insights
Settings
Overview
Reporting
Policy
Advisories
Vulnerability alerts
Dependabot 1
Code scanning 11
Secret scanning
Code scanning
All tools are working as expected
Tool status 1
Add tool
is:open branch:main
11 Open
0 Closed
Language
Tool
Branch
Rule
Severity
Sort
Ensure rotation for customer created CMKs is enabled
Error
#7 opened 3 hours ago • Detected by terrascan in file:/.../gregsienkiewicz/reimagined-broccoli.git:1
main
Security Groups - Unrestricted Specific Ports - (HTTP,80)
Error
#5 opened 3 hours ago • Detected by terrascan in file:/.../gregsienkiewicz/reimagined-broccoli.git:160
main
Security Groups - Unrestricted Specific Ports - Prevalent known internal port (TCP,3000)
Error
#2 opened 3 hours ago • Detected by terrascan in file:/.../gregsienkiewicz/reimagined-broccoli.git:126
main
Ensure ECR repository is encrypted at rest
Warning
#11 opened 3 hours ago • Detected by terrascan in file:/.../gregsienkiewicz/reimagined-broccoli.git:1
main
Ensure AWS Cloudwatch log group has retention policy set.
Warning
#10 opened 3 hours ago • Detected by terrascan in file:/.../gregsienkiewicz/reimagined-broccoli.git:6
main
Ensure Point In Time Recovery is enabled for DynamoDB Tables
Warning
#9 opened 3 hours ago • Detected by terrascan in file:/.../gregsienkiewicz/reimagined-broccoli.git:27
main
Ensure ECR repository has policy attached.
Warning
#6 opened 3 hours ago • Detected by terrascan in file:/.../gregsienkiewicz/reimagined-broccoli.git:1
main
Ensure DynamoDb is encrypted at rest
Warning
#4 opened 3 hours ago • Detected by terrascan in file:/.../gregsienkiewicz/reimagined-broccoli.git:27
main
Ensure Target Group use HTTPs to ensure end to end encryption
Warning
#3 opened 3 hours ago • Detected by terrascan in file:/.../gregsienkiewicz/reimagined-broccoli.git:9
main
Ensure there is a listener configured on HTTPs or with a port 443
Warning
#1 opened 3 hours ago • Detected by terrascan in file:/.../gregsienkiewicz/reimagined-broccoli.git:21
main

Backup Your Data!

… shameless plug.

Marketplace

Type / to search

Extend GitHub

Add tools to help you build and grow

Explore apps | Contact Sales

Types

- Apps
- Actions

Categories

- API management
- Chat
- Code quality
- Code review
- Continuous integration
- Dependency management

Search for apps and actions

Sort: Best Match

Apps

Rewind Backups for GitHub (Formerly BackHub)
By backhub
Automatic daily backups of your GitHub repos and metadata with on-demand restores to protect your business
Recommended

CircleCI
By circleci
Automatically build, test, and deploy your project in minutes
Recommended

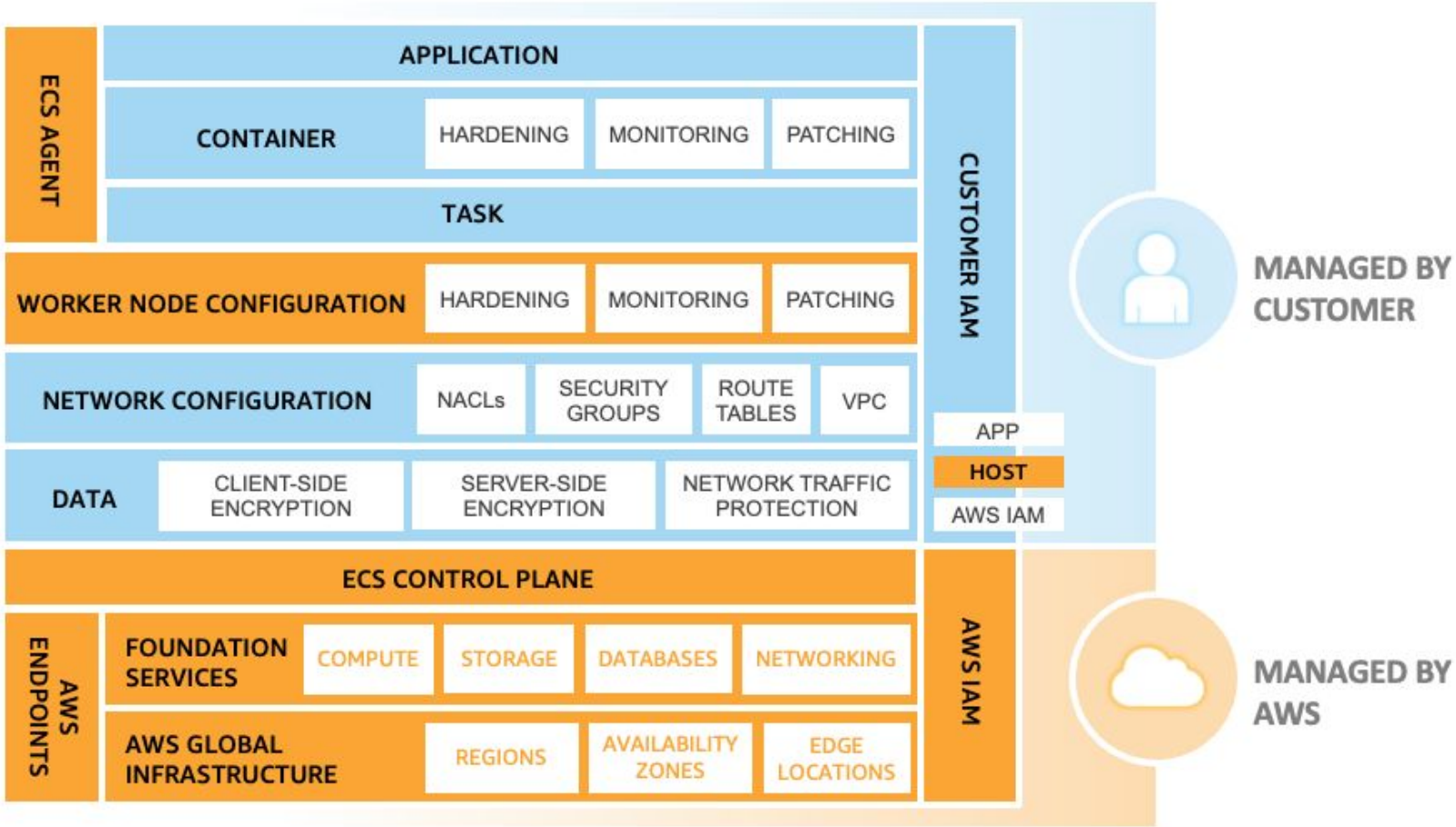
Imgbot
By imgbot
A GitHub app that optimizes your images

CodeFactor
By codefactor-io
Automated code review for GitHub

AWS

Protect the runtime.

AWS Shared Responsibility Model for Amazon ECS with Fargate



Secure the ECS task and runtime

Secure your container’s images


Scan your container's images using Amazon Inspector
Amazon Inspector creates an event for Amazon EventBridge for malicious findings
Amazon SNS sends notifications to the concerned parties
Amazon Elastic Container Registry
Amazon Inspector
Amazon EventBridge
Amazon SNS

TODO Add Private Registry scan config screengrab

Amazon Elastic Container Registry

Private registry
Public registry
Repositories
- Summary
- Images
- Permissions
- Lifecycle Policy
- Repository tags

ECR public gallery
Amazon ECS
Amazon EKS

Getting started
Documentation

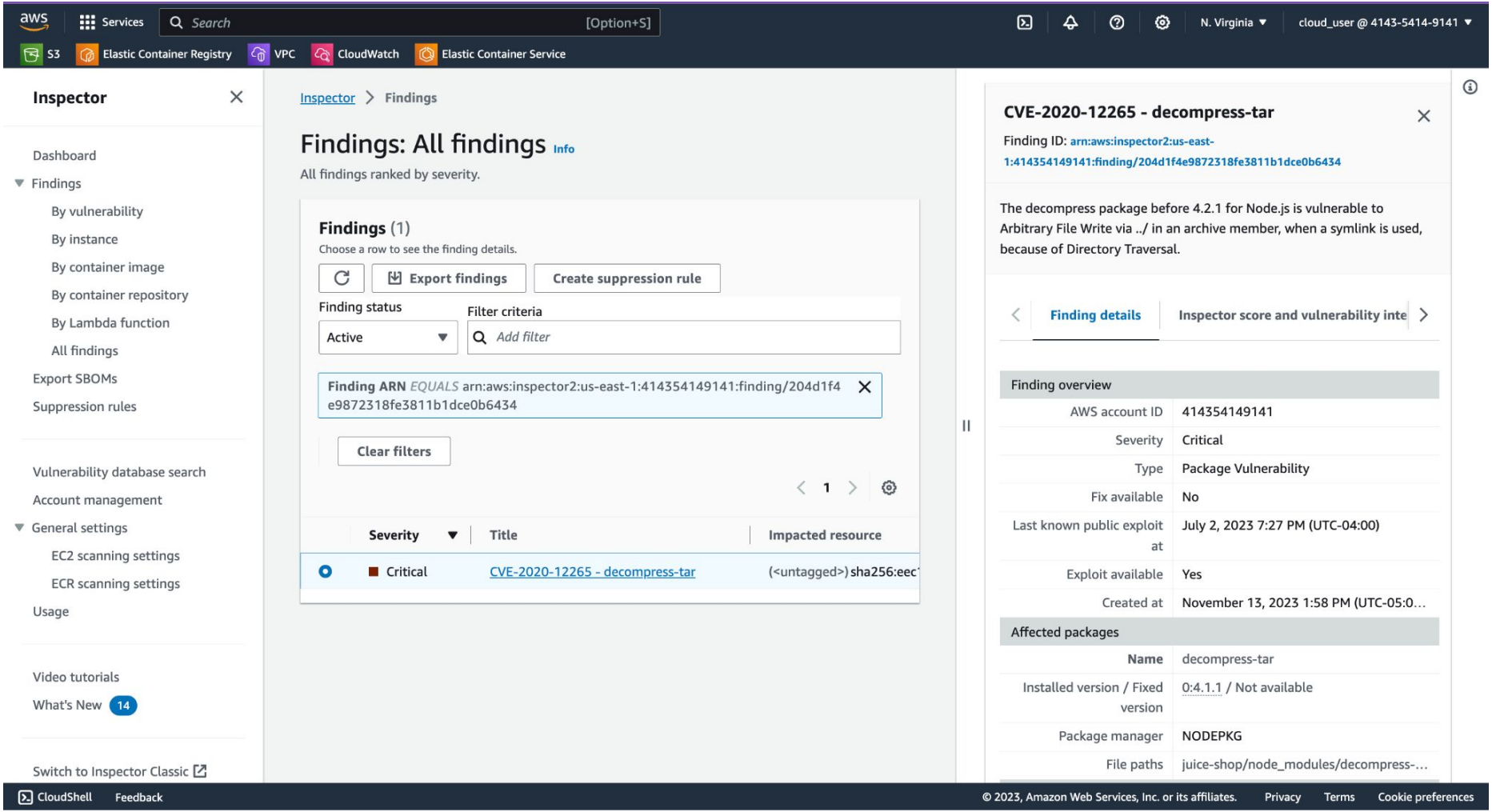
Overview

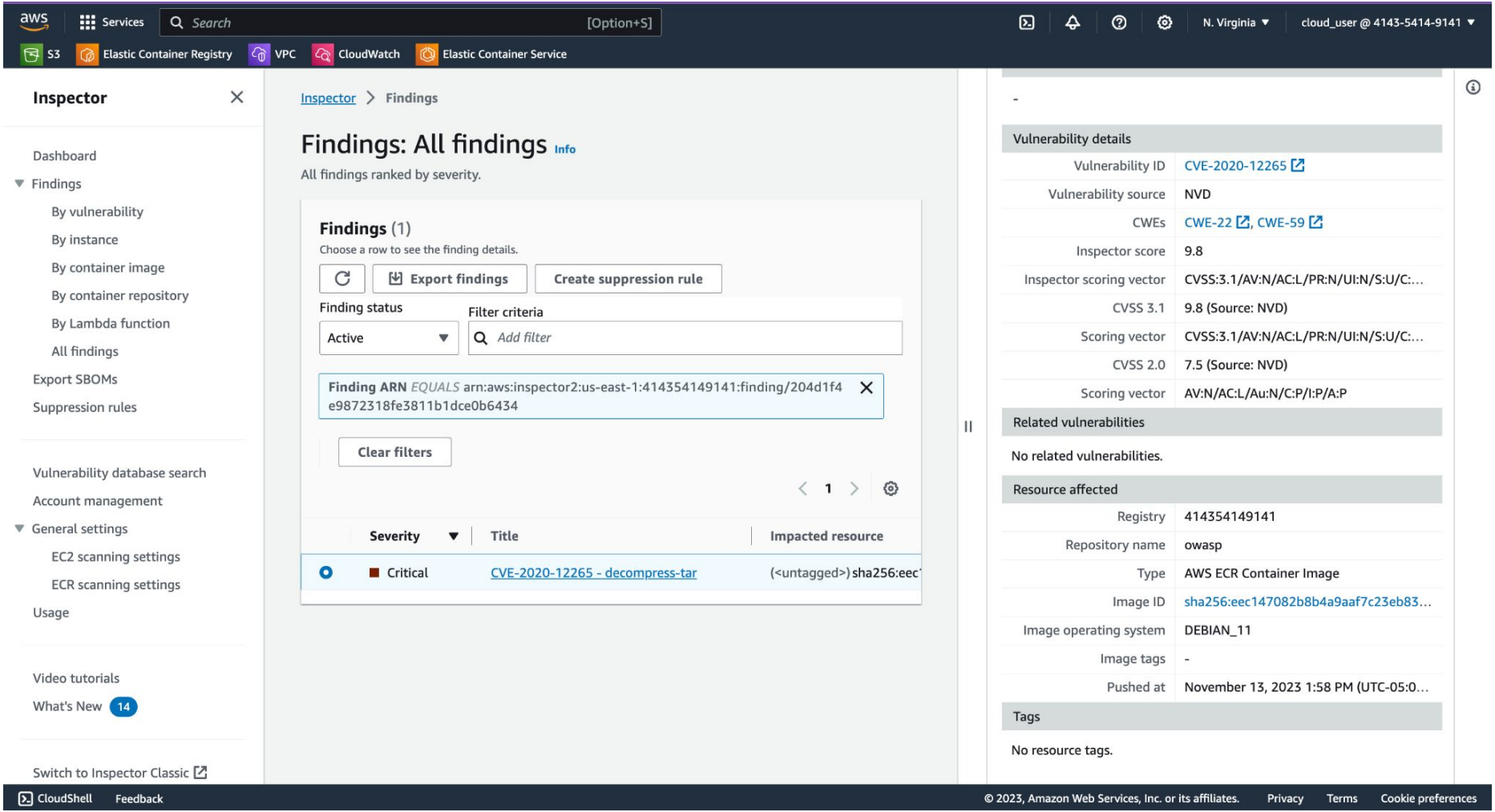
Critical	High	Medium	Low	Informational	Undefined
12	21	22	1	0	0

Vulnerabilities (56)

1

Name	Package	Severity	Description	Status	Remediation
SNYK-JS-SANITIZEHTML-585892	sanitize-html	CRITICAL	## Overview [sanitize-html](https://github.com/punkave/sanitize-html) is a library that allows you to clean up user-submitted HTML, preserving whitelisted elements and whitelisted attributes on a per-element basis Affected versions of this package are vulnerable to Arbitrary Code Execution. Tag transformations which turn an attribute value into a text node using `transformTags` could be vulnerable to code execution. ## Remediation Upgrade `sanitize-html` to version 2.0.0-beta or higher. ## References - [GitHub PR](https://github.com/apostrophecms/sanitize-html/pull/156)	ACTIVE	None Provided
CVE-2020-12265	decompress-tar	CRITICAL	The decompress package before 4.2.1 for Node.js is vulnerable to Arbitrary File Write via ../ in an archive member, when a symlink is used, because of Directory Traversal.	ACTIVE	None Provided
			In express-jwt (NPM package) up and including version 5.3.3, the algorithms		


aws
Services
Search
[Option+S]
N. Virginia
cloud_user @ 4143-5414-9141
S3
Elastic Container Registry
VPC
CloudWatch
Elastic Container Service
Inspector
Dashboard
Findings
By vulnerability
By instance
By container image
By container repository
By Lambda function
All findings
Export SBOMs
Suppression rules
Vulnerability database search
Account management
General settings
EC2 scanning settings
ECR scanning settings
Usage
Video tutorials
What's New 14
Switch to Inspector Classic
Inspector > Findings
Findings: All findings Info
All findings ranked by severity.
Findings (1)
Choose a row to see the finding details.
Export findings
Create suppression rule
Finding status
Active
Filter criteria
Add filter
Finding ARN EQUALS arn:aws:inspector2:us-east-1:414354149141:finding/204d1f4e9872318fe3811b1dce0b6434
Clear filters
1
Severity
Title
Impacted resource
Critical
CVE-2020-12265 - decompress-tar
(<untagged>) sha256:eec
CVE-2020-12265 - decompress-tar
Finding ID: arn:aws:inspector2:us-east-1:414354149141:finding/204d1f4e9872318fe3811b1dce0b6434
The decompress package before 4.2.1 for Node.js is vulnerable to Arbitrary File Write via ../ in an archive member, when a symlink is used, because of Directory Traversal.
Finding details
Inspector score and vulnerability inte
Finding overview
AWS account ID 414354149141
Severity Critical
Type Package Vulnerability
Fix available No
Last known public exploit at July 2, 2023 7:27 PM (UTC-04:00)
Exploit available Yes
Created at November 13, 2023 1:58 PM (UTC-05:0…
Affected packages
Name decompress-tar
Installed version / Fixed version 0:4.1.1 / Not available
Package manager NODEPKG
File paths juice-shop/node_modules/decompress-…
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Option+S]
N. Virginia
cloud_user @ 4143-5414-9141
S3
Elastic Container Registry
VPC
CloudWatch
Elastic Container Service
Inspector
Dashboard
Findings
By vulnerability
By instance
By container image
By container repository
By Lambda function
All findings
Export SBOMs
Suppression rules
Vulnerability database search
Account management
General settings
EC2 scanning settings
ECR scanning settings
Usage
Video tutorials
What's New 14
Switch to Inspector Classic
Inspector > Findings
Findings: All findings Info
All findings ranked by severity.
Findings (1)
Choose a row to see the finding details.
Export findings
Create suppression rule
Finding status
Active
Filter criteria
Add filter
Finding ARN EQUALS arn:aws:inspector2:us-east-1:414354149141:finding/204d1f4e9872318fe3811b1dce0b6434
Clear filters
1
Severity
Title
Impacted resource
Critical
CVE-2020-12265 - decompress-tar
(<untagged>) sha256:eec
-
Vulnerability details
Vulnerability ID CVE-2020-12265
Vulnerability source NVD
CWEs CWE-22, CWE-59
Inspector score 9.8
Inspector scoring vector CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:...
CVSS 3.1 9.8 (Source: NVD)
Scoring vector CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:...
CVSS 2.0 7.5 (Source: NVD)
Scoring vector AV:N/AC:L/Au:N/C:P/I:P/A:P
Related vulnerabilities
No related vulnerabilities.
Resource affected
Registry 414354149141
Repository name owasp
Type AWS ECR Container Image
Image ID sha256:eec147082b8b4a9aaf7c23eb83...
Image operating system DEBIAN_11
Image tags -
Pushed at November 13, 2023 1:58 PM (UTC-05:0...
Tags
No resource tags.
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Secure the ECS task and runtime

Enable the ECR tag immutability feature

TODO Add Private Registry configuration screen grab

TODO Add push failure on tag immutability

TODO Add right way to push

Secure the ECS task and runtime

Secure your containers and tasks

TODO Add container definition screen grab

Multi stage build

TODO Add container definition screen grab

Multi stage build

Thank you.

OWASP Ottawa organizers and volunteers.

University of Ottawa

All my great colleagues at Rewind.