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

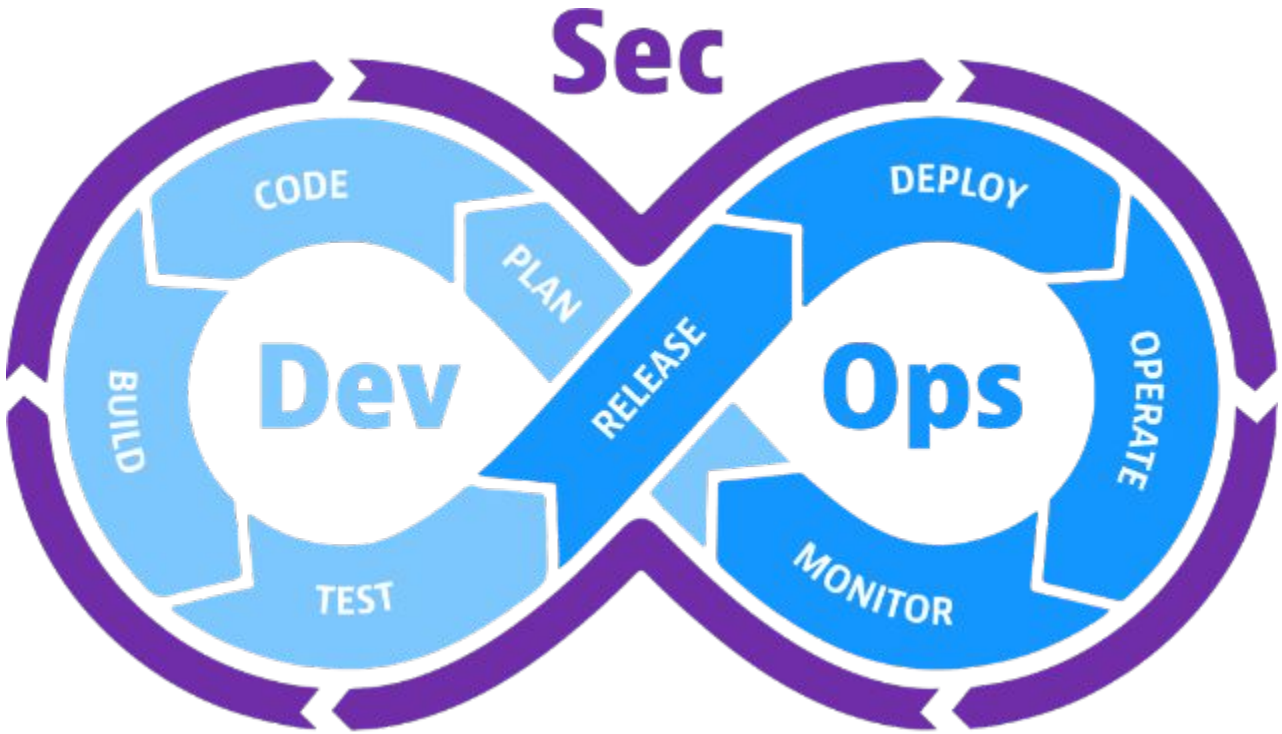
Book a demo >

Trusted by over 100,000 organizations across the globe.

Glossier. HBO MailOnline Amplitude MOOMIN OLAPLEX.

DevSecOps?

Supreme Allied Commander SDLC Force (SACSDLC)


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

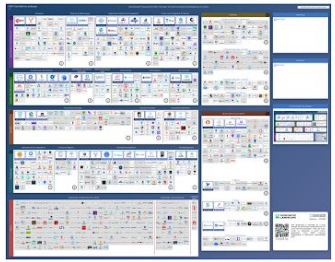
Capital One, ebay, Fidelity, JPMorgan Chase & Co., NGINX, salesforce

General

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

Associate

CNCF Landscape



CNCF Technical Advisory Group (TAG) for Security

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

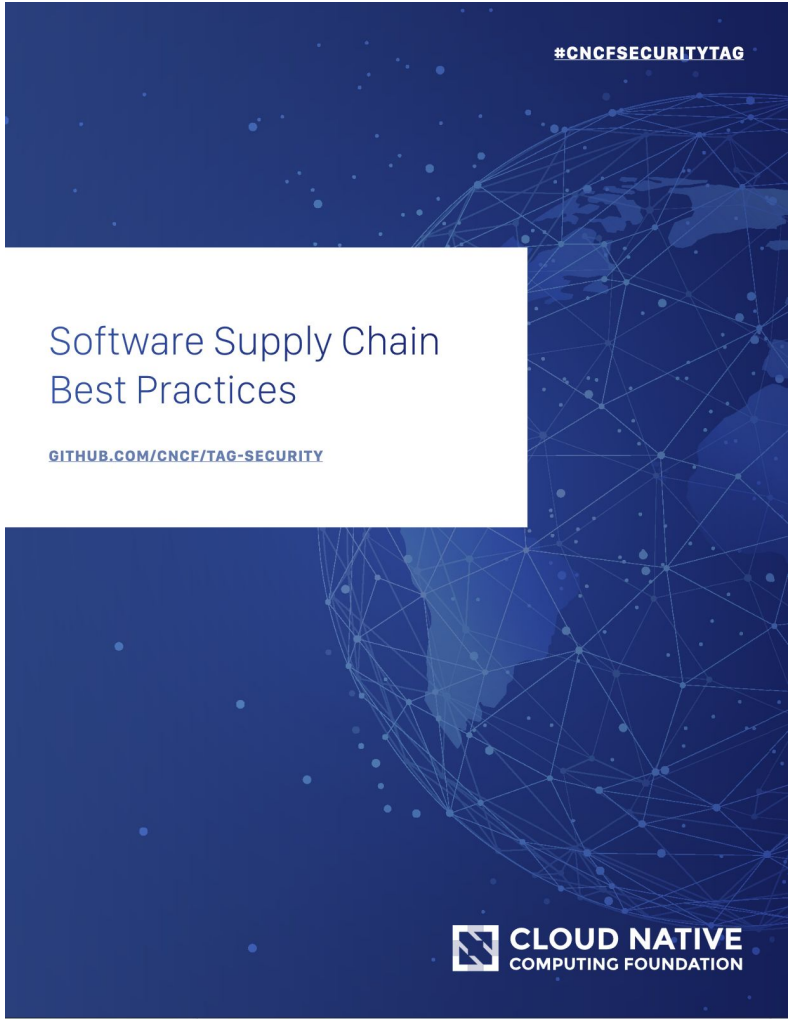
• Securing the Source Code: securing code produced by software producers (the internal or first party code)

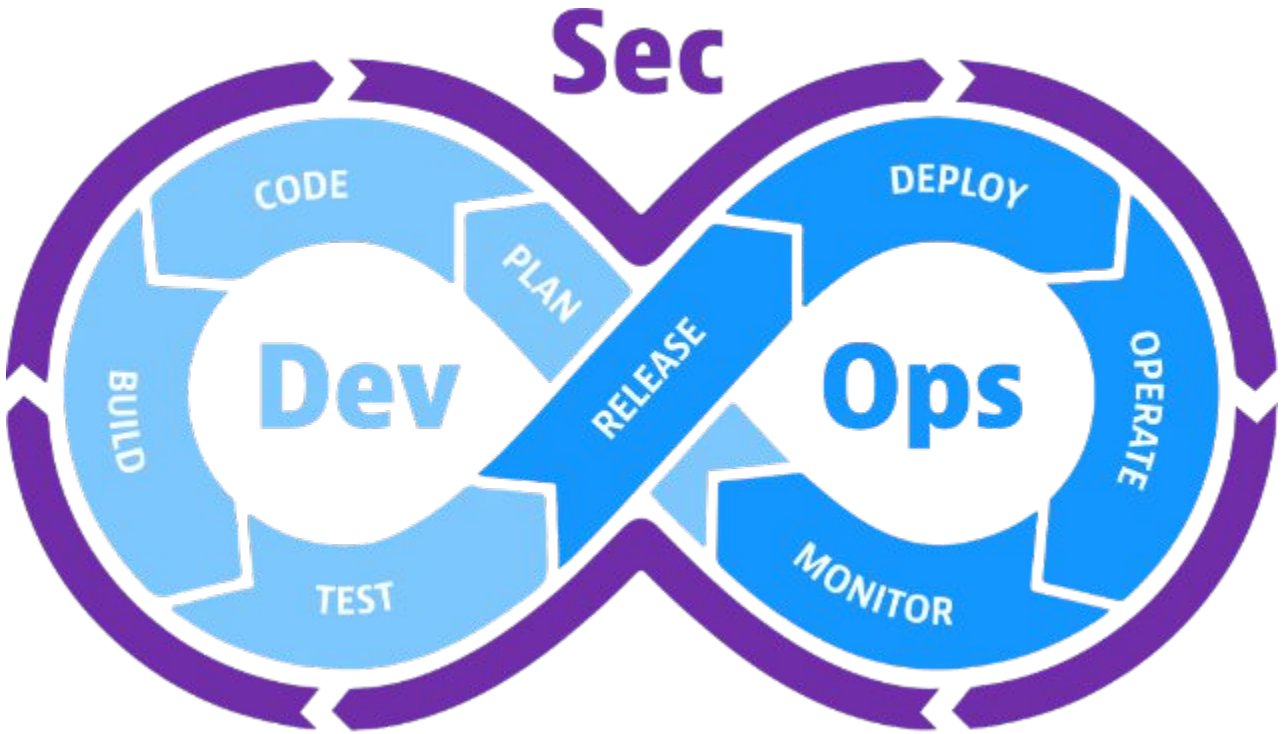
• Securing the Materials: hardening the “raw materials” of second and third party code incorporated in builds

• 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

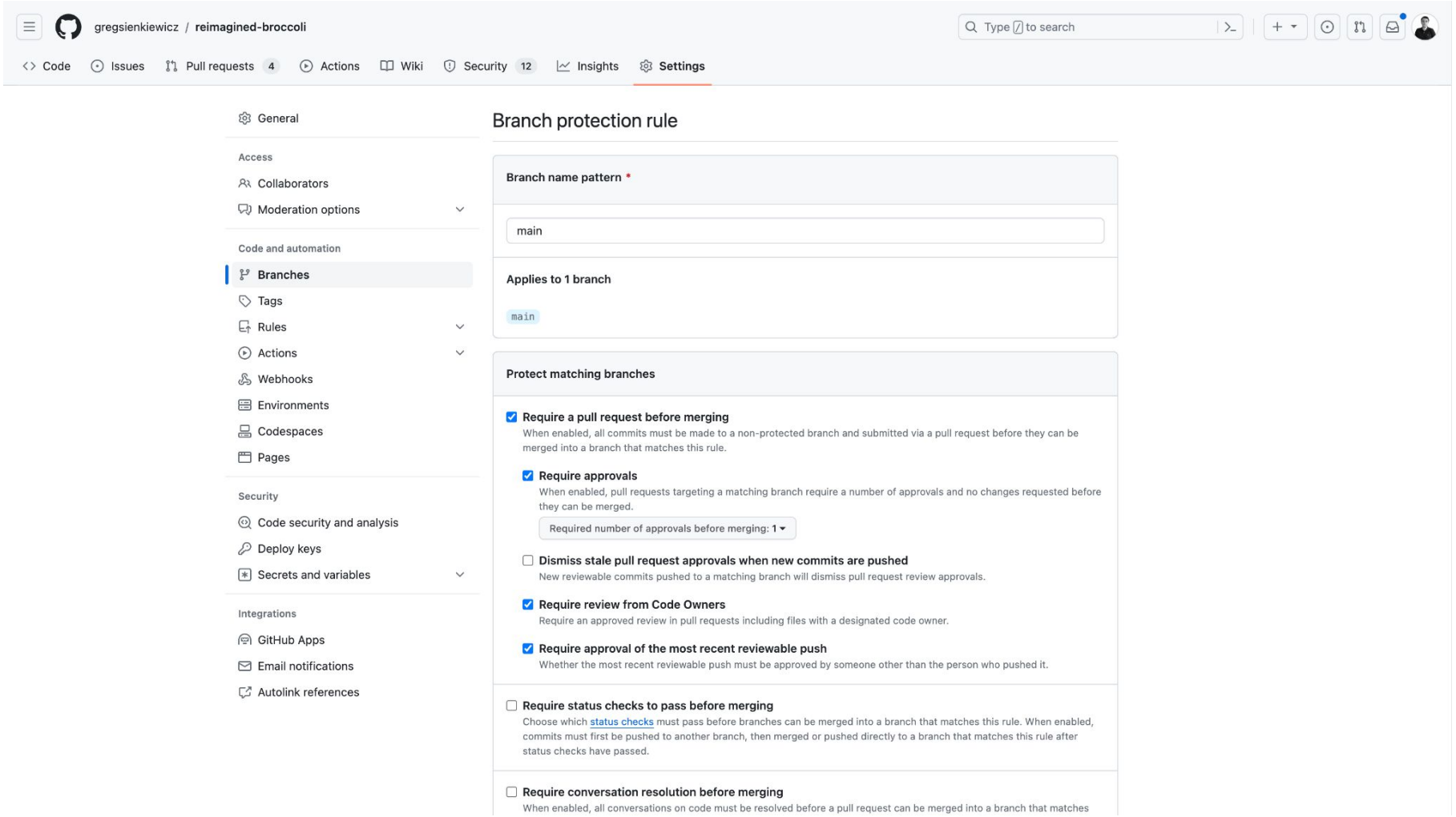
“It’s not the Destination. It's the journey.”

Ralph Waldo Emerson (disputed but works in this context)

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

Commits

main

Commits on Nov 14, 2023

refactor: Remove bridgecrewio/checkov-action workflow (#12)
gregsienkiewicz committed now
Verified 2bd7bbe

fix: Remove AWS credentials (#11)
gregsienkiewicz committed 9 minutes ago
Verified 8085e10

Update CODEOWNERS
gregsienkiewicz committed 6 hours ago
Verified 65dde58

feature: Add CODEOWNERS (#10)
gregsienkiewicz committed 6 hours ago
Verified cce6c74

fix: GitHub Action refactoring (#6)
gregsienkiewicz committed 8 hours ago
Verified 5aa6703

Commits on Nov 12, 2023

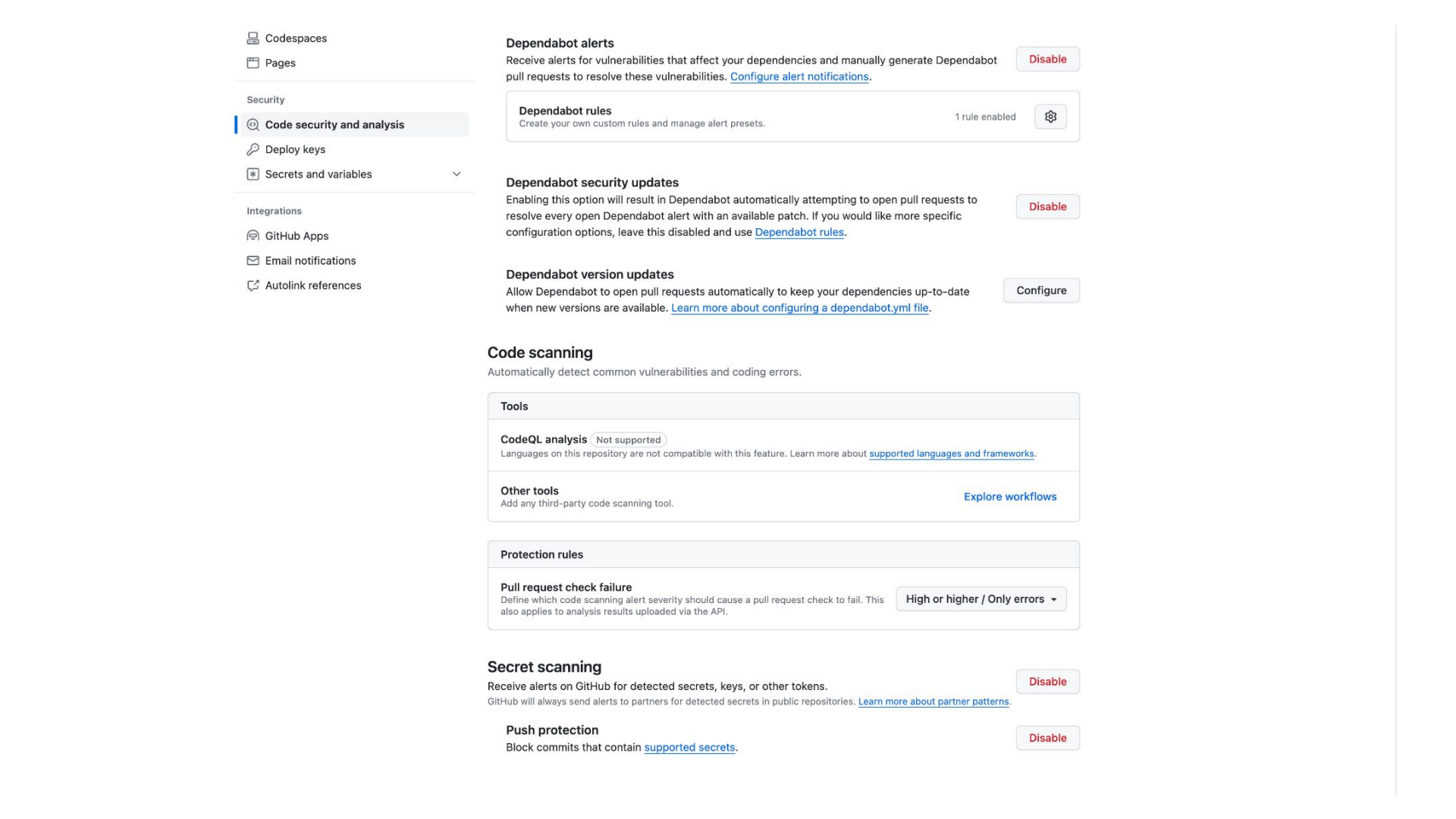
feature: Add AWS resources (#4)
gregsienkiewicz committed 2 days ago
Verified eb1a545

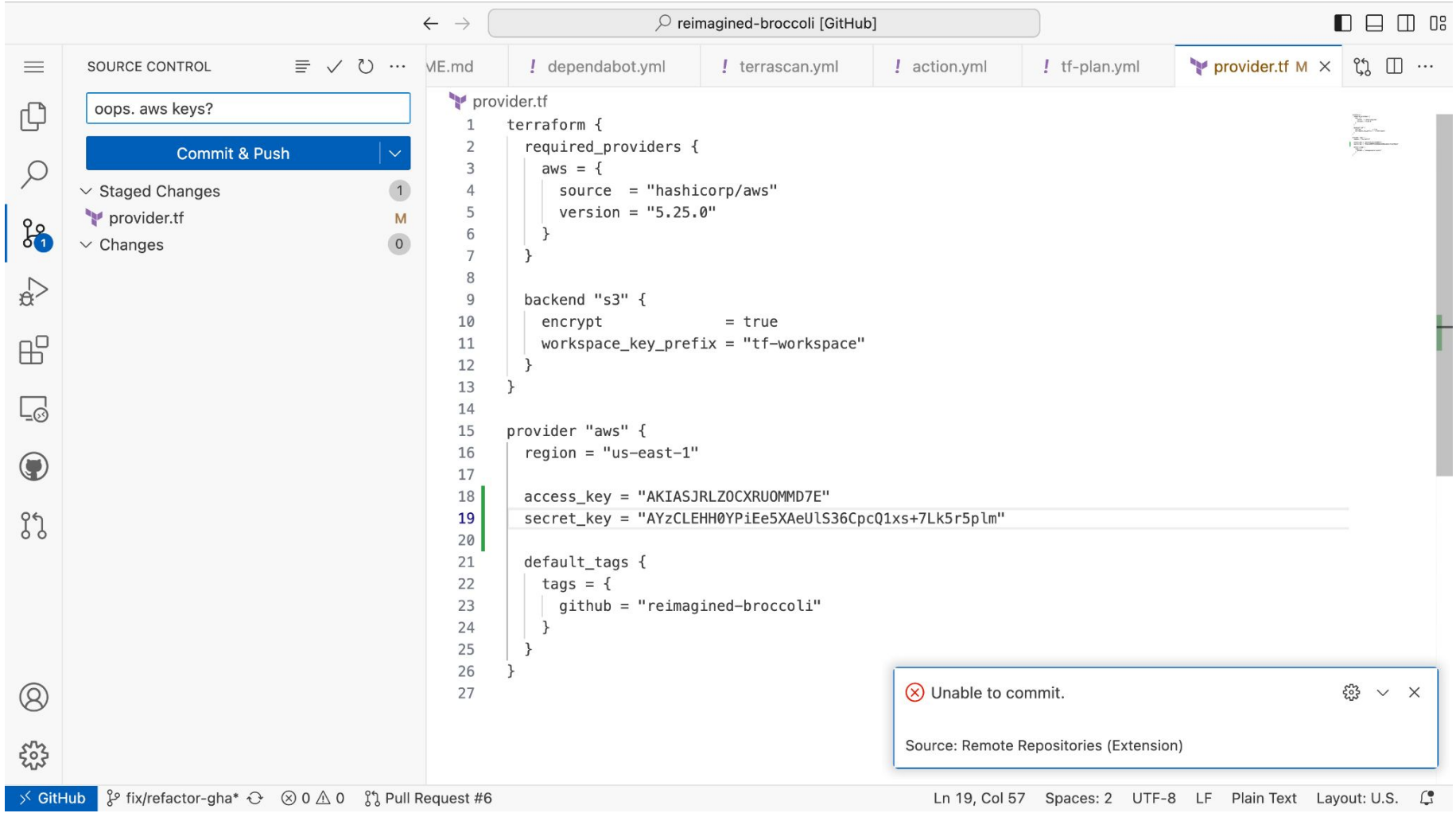
feature: GitHub actions (#1)
gregsienkiewicz committed 2 days ago
Verified 2ec6ef3

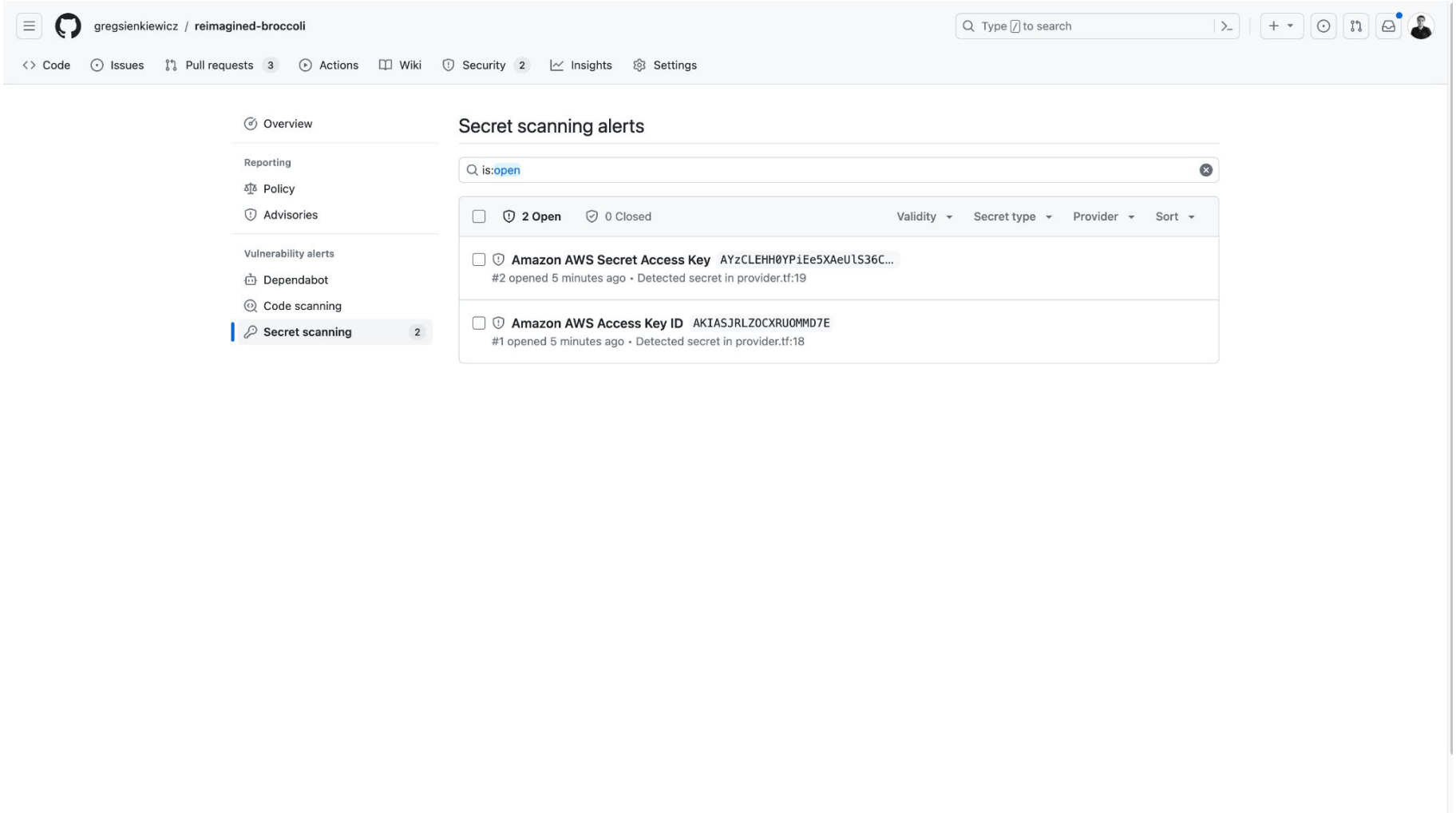
Commits on Nov 7, 2023

Initial commit
gregsienkiewicz committed last week
Verified 928337b

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

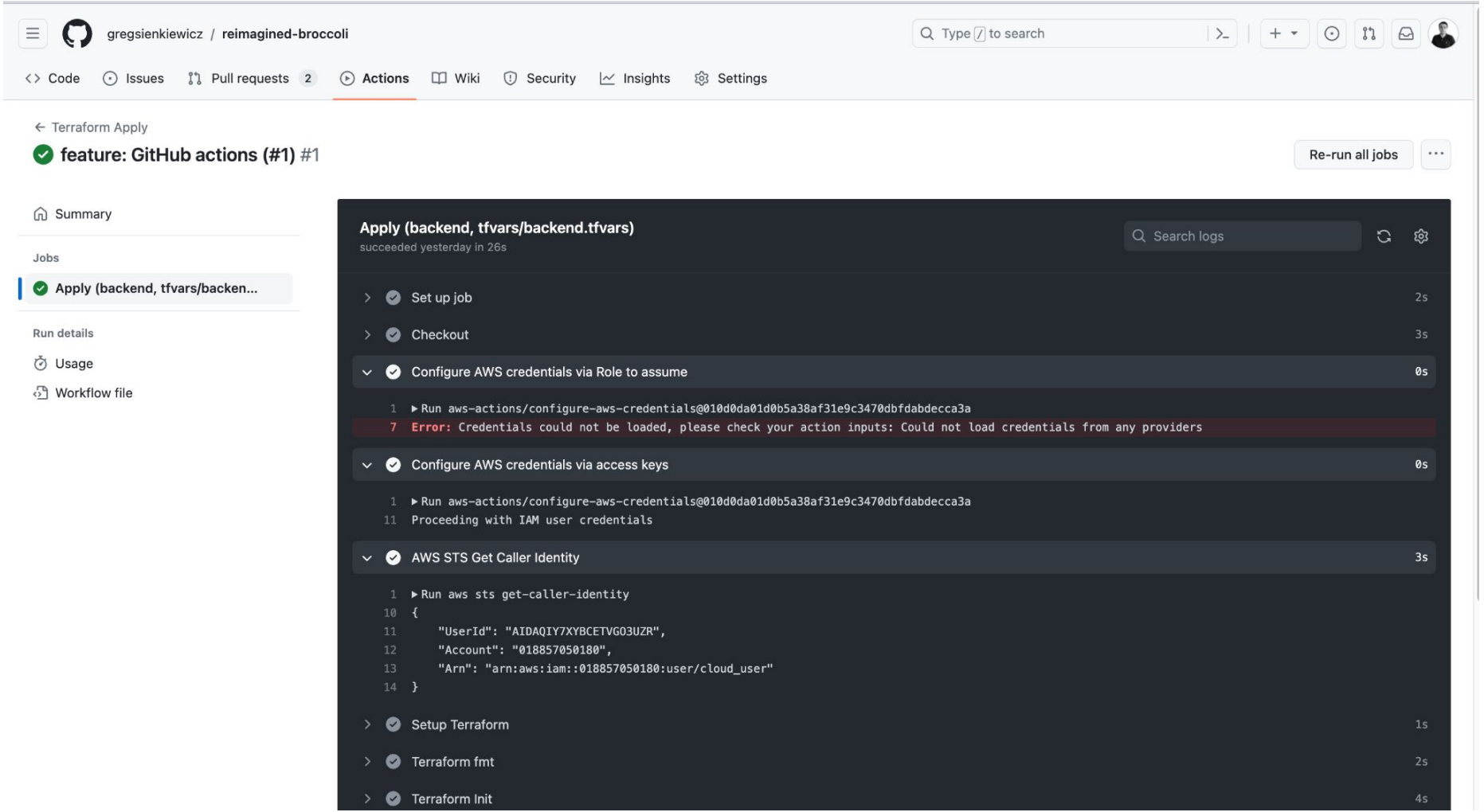
reimagined-broccoli / .github / workflows / tf-plan.yml

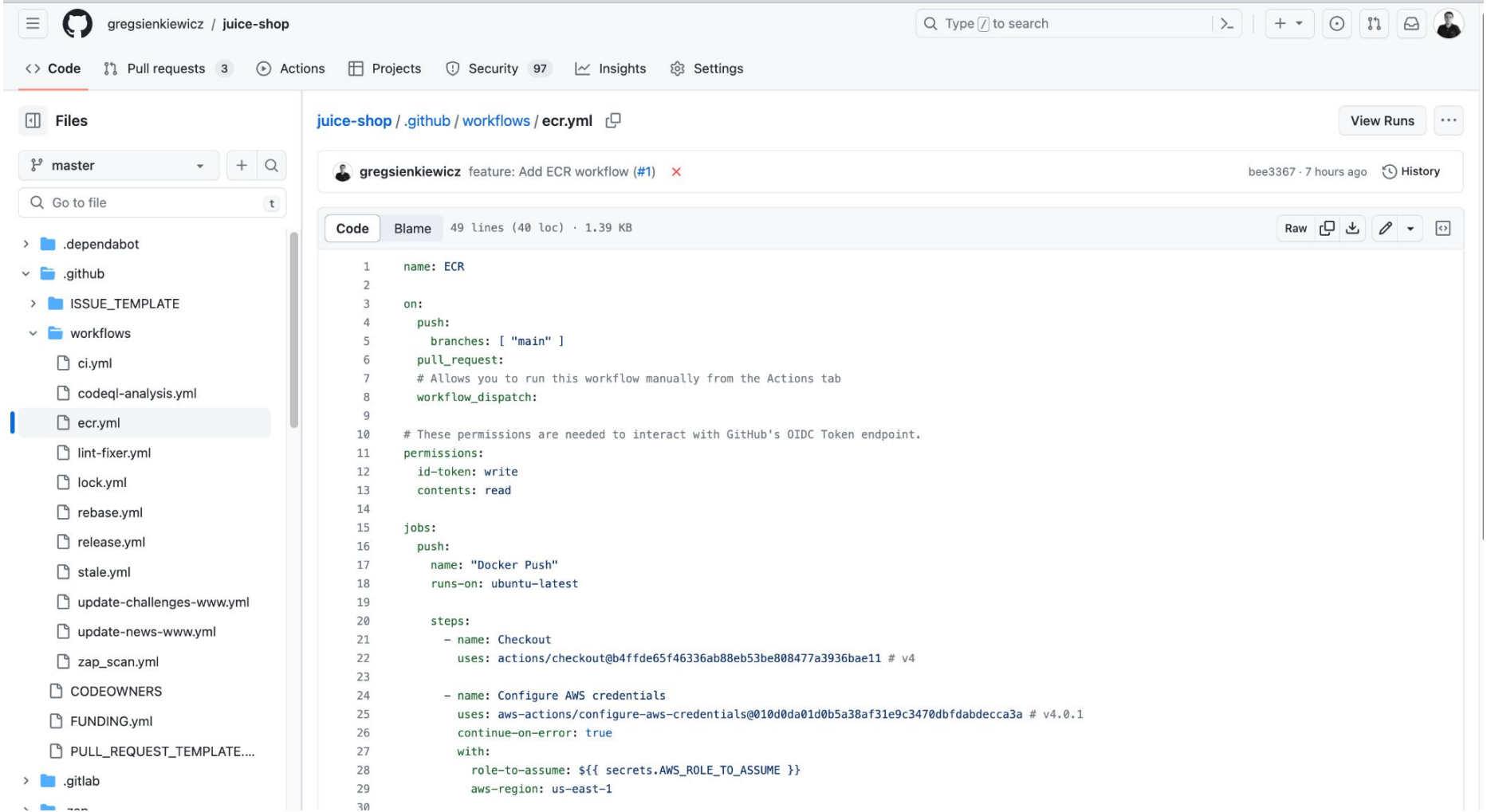
Top

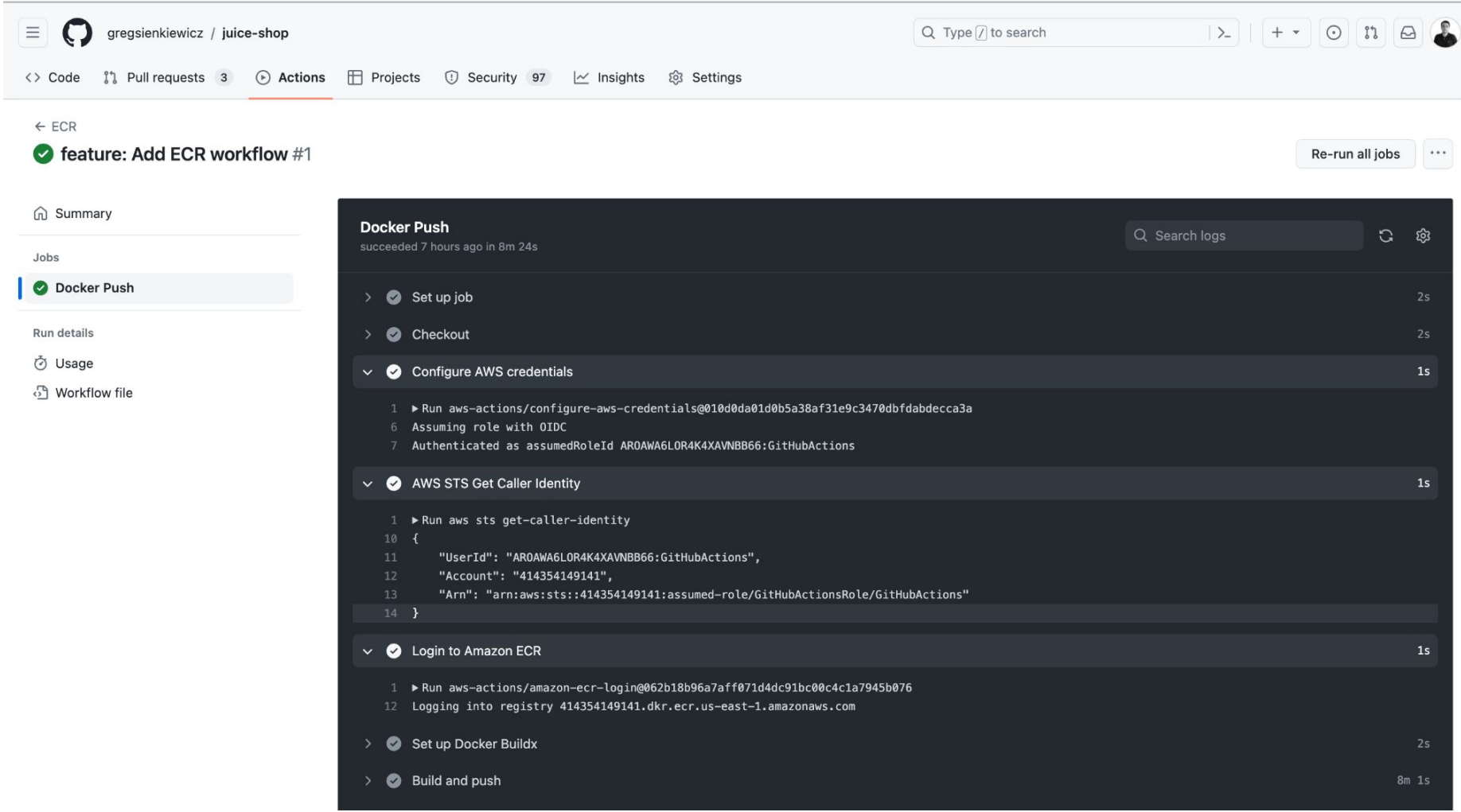
Code Blame 109 lines (86 loc) · 3.27 KB

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 }
```

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management
User groups
Users
Roles
Policies
Identity providers
Account settings

Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)

Related consoles
IAM Identity Center

IAM > Identity providers > token.actions.githubusercontent.com

token.actions.githubusercontent.com Info

Assign role | Delete

Summary

Provider	Provider Type	Creation Time	ARN
token.actions.githubusercontent.com	OpenID Connect	November 14, 2023, 21:13 (UTC-05:00)	arn:aws:iam::131185384471:oidc-provider/token.actions.githubusercontent.com

Audiences (1)

Actions

Also known as client ID, audience is a value that identifies the application that is registered with an OpenID Connect provider.

1

Audience
sts.amazonaws.com

Thumbprints (2)

Manage

Server certificate thumbprint is the hex-encoded SHA-1 hash value of the X.509 certificate used by the domain where the OpenID Connect provider makes its keys available.

You can add up to 5 thumbprints. This lets you maintain multiple thumbprints if the identity provider is rotating certificates.

⚠ AWS secures communication with this OIDC identity provider (IdP) using our library of trusted CAs rather than using a certificate thumbprint to verify the server certificate of your IdP. Your legacy thumbprint(s) will remain in your configuration but will no longer be needed for validation.

6938fd4d98bab03faadb97b34396831e3780aea1

1c58a3a8518e8759bf075b76b750d4f2df264fcd

Tags (1)

Manage tags

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management
User groups
Users
Roles
Policies
Identity providers
Account settings

Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)

Related consoles
IAM Identity Center
AWS Organizations

GitHubActionsRole Info

Delete

Summary

Edit

Creation date
November 14, 2023, 21:13 (UTC-05:00)

ARN
arn:aws:iam::131185384471:role/GitHubActionsRole

Last activity
-

Maximum session duration
1 hour

Permissions | Trust relationships | Tags (1) | Access Advisor | Revoke sessions

Trusted entities

Edit trust policy

Entities that can assume this role under specified conditions.


```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Federated": "arn:aws:iam::131185384471:oidc-provider/token.actions.githubusercontent.com"
            },
            "Action": "sts:AssumeRoleWithWebIdentity",
            "Condition": {
                "ForAllValues:StringEquals": {
                    "token.actions.githubusercontent.com:aud": "sts.amazonaws.com",
                    "token.actions.githubusercontent.com:iss": "https://token.actions.githubusercontent.com"
                },
                "ForAnyValue:StringLike": {
                    "token.actions.githubusercontent.com:sub": [
                        "repo:juice-shop/juice-shop:*",
                        "repo:gregsienkiewicz/reimagined-broccoli:*",
                        "repo:gregsienkiewicz/juice-shop:*"
                    ]
                }
```

CloudTrail

Dashboard
Event history
Insights
Lake
Dashboard New
Query
Event data stores
Integrations
Trails

Settings

Pricing
Documentation
Forums
FAQs

GetAuthorizationToken Info

Details Info

Event time November 14, 2023, 21:37:51 (UTC-05:00)	AWS access key ASIAR5C2CDQL6OK4UXPB	AWS region us-east-1
User name GitHubActions	Source IP address 20.172.7.23	Error code -
Event name GetAuthorizationToken	Event ID e5986a87-f112-4a25-b2fd-970b7a642eae	Read-only true
Event source ecr.amazonaws.com	Request ID 552a1fa7-54e0-4555-a2aa-39eb083ea483	

Resources referenced (0) Info

Resource type	Resource name	AWS Config resource timeline
No resources referenced		

Event record Info

Copy

JSON view


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAR5C2CDQLTBAEF2JVW:GitHubActions",
        "arn": "arn:aws:sts::131185384471:assumed-role/GitHubActionsRole/GitHubActions",
        "accountId": "131185384471",
        "accessKeyId": "ASIAR5C2CDQL6OK4UXPB",
```

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

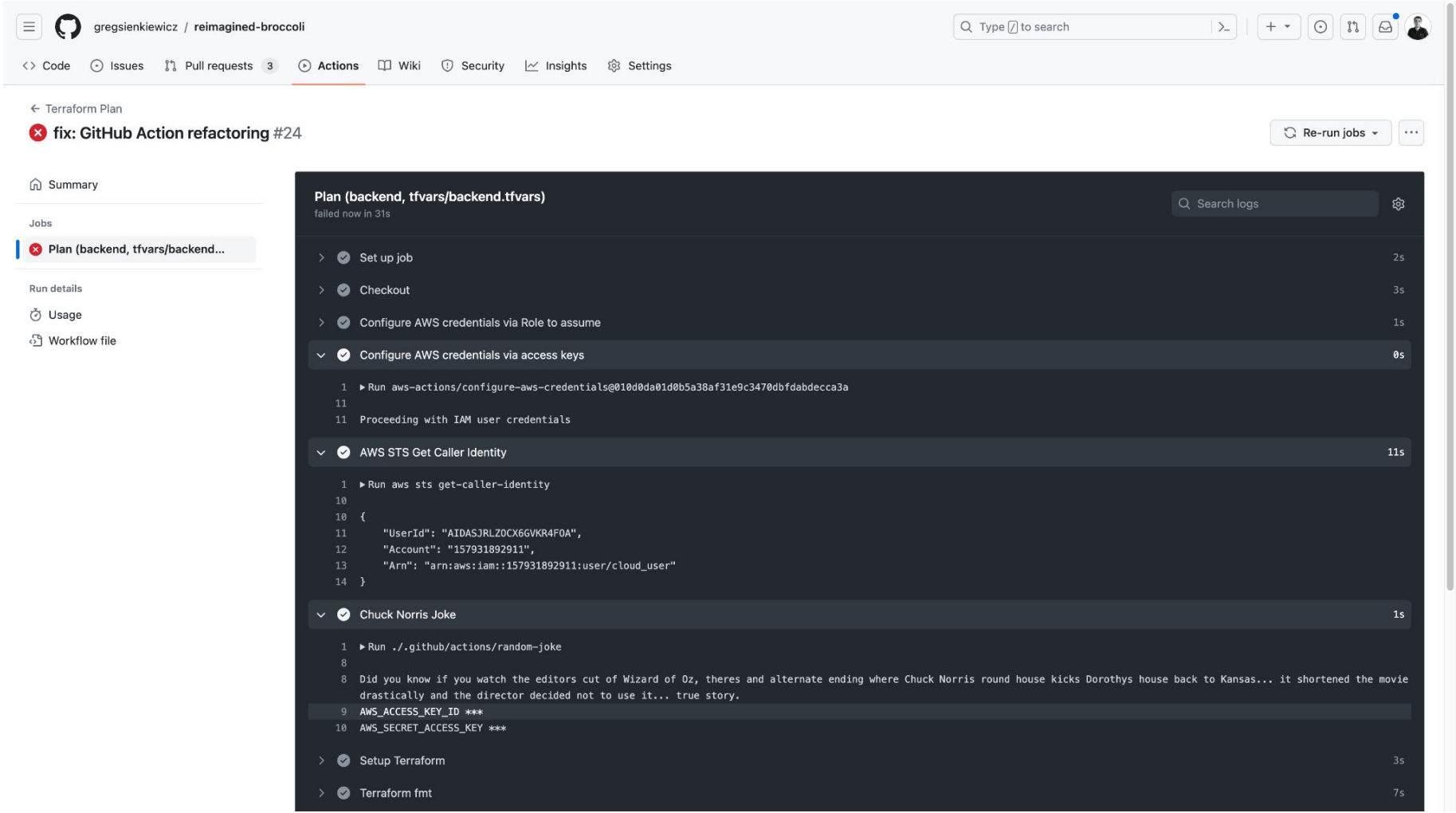
- .github
  - actions/random-joke
  - workflows
    - checkov.yml
    - terrascan.yml
    - tf-apply.yml
    - tf-plan.yml
  - dependabot.yml
- task-definitions
- tfvars
- .gitignore
- LICENSE
- README.md
- alb.tf
- backend.tf
- cloudwatch.tf
- ecr.tf
- ecr_lifecycle_policy.json
- ecs.tf
- github_oidc.tf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

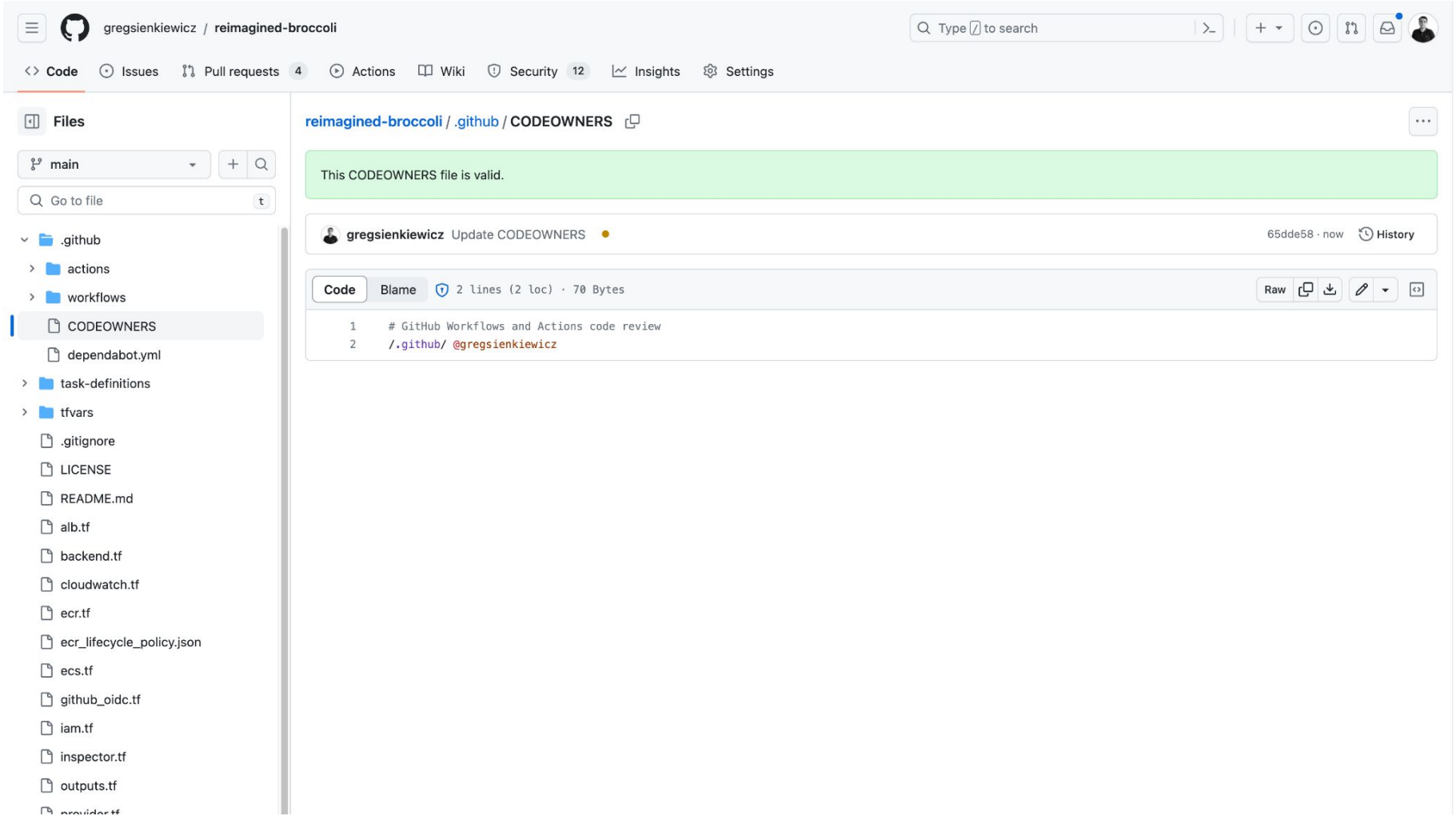
reimagined-broccoli / .github / actions / random-joke / **gha.js**

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

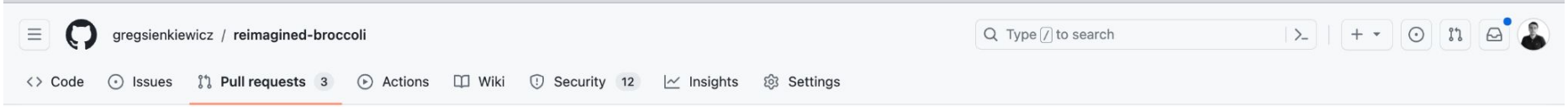
Documentation • Share feedback

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 3
Actions
Wiki
Security 12
Insights
Settings
Filters
is:pr is:open
Labels 9
Milestones 0
New pull request
3 Open
9 Closed
Author
Label
Projects
Milestones
Reviews
Assignee
Sort
build(deps): bump actions/github-script from 6 to 7
#9 opened 9 hours ago by dependabot bot • Review required
1
build(deps): bump tenable/terrascan-action from 1.4.1 to 1.5.0
#8 opened 9 hours ago by dependabot bot • Review required
1
build(deps): bump hashicorp/setup-terraform from 2 to 3
#2 opened 2 days ago by dependabot bot • Review required
2
ProTip! Type g i on any issue or pull request to go back to the issue listing page.
© 2023 GitHub, Inc.
Terms
Privacy
Security
Status
Docs
Contact GitHub
Pricing
API
Training
Blog
About

build(deps): bump hashicorp/setup-terraform from 2 to 3 #2

Edit Code

Open **dependabot** wants to merge 1 commit into `main` from `dependabot/github_actions/hashicorp/setup-terraform-3`

Conversation 2 Commits 1 Checks 5 Files changed 2 +2 −2

dependabot bot commented on behalf of **github** 3 days ago • edited

Bumps hashicorp/setup-terraform from 2 to 3.

▼ Release notes

Sourced from hashicorp/setup-terraform's releases.

v3.0.0

NOTES:

- Updated default runtime to node20 (#346)
- The wrapper around the installed Terraform binary has been fixed to return the exact STDOUT and STDERR from Terraform when executing commands. Previous versions of setup-terraform may have required workarounds to process the STDOUT in bash, such as filtering out the first line or selectively parsing STDOUT with jq. These workarounds may need to be adjusted with `v3.0.0`, which will now return just the STDOUT/STDERR from Terraform with no errant characters/statements. (#367)

BUG FIXES:

- Fixed malformed stdout when wrapper is enabled (#367)

v2.0.3

What's Changed

NOTES

- Bump `@actions/core` from 1.9.1 to 1.10.0 by `@dependabot` in hashicorp/setup-terraform#247

Full Changelog: hashicorp/setup-terraform@ `v2.0.2...v2.0.3`

Reviewers

Suggestions

gregsienkiewicz Request

At least 1 approving review is required to merge this pull request.

Still in progress? Convert to draft

Assignees

No one—assign yourself

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

Notifications Customize

Unsubscribe

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

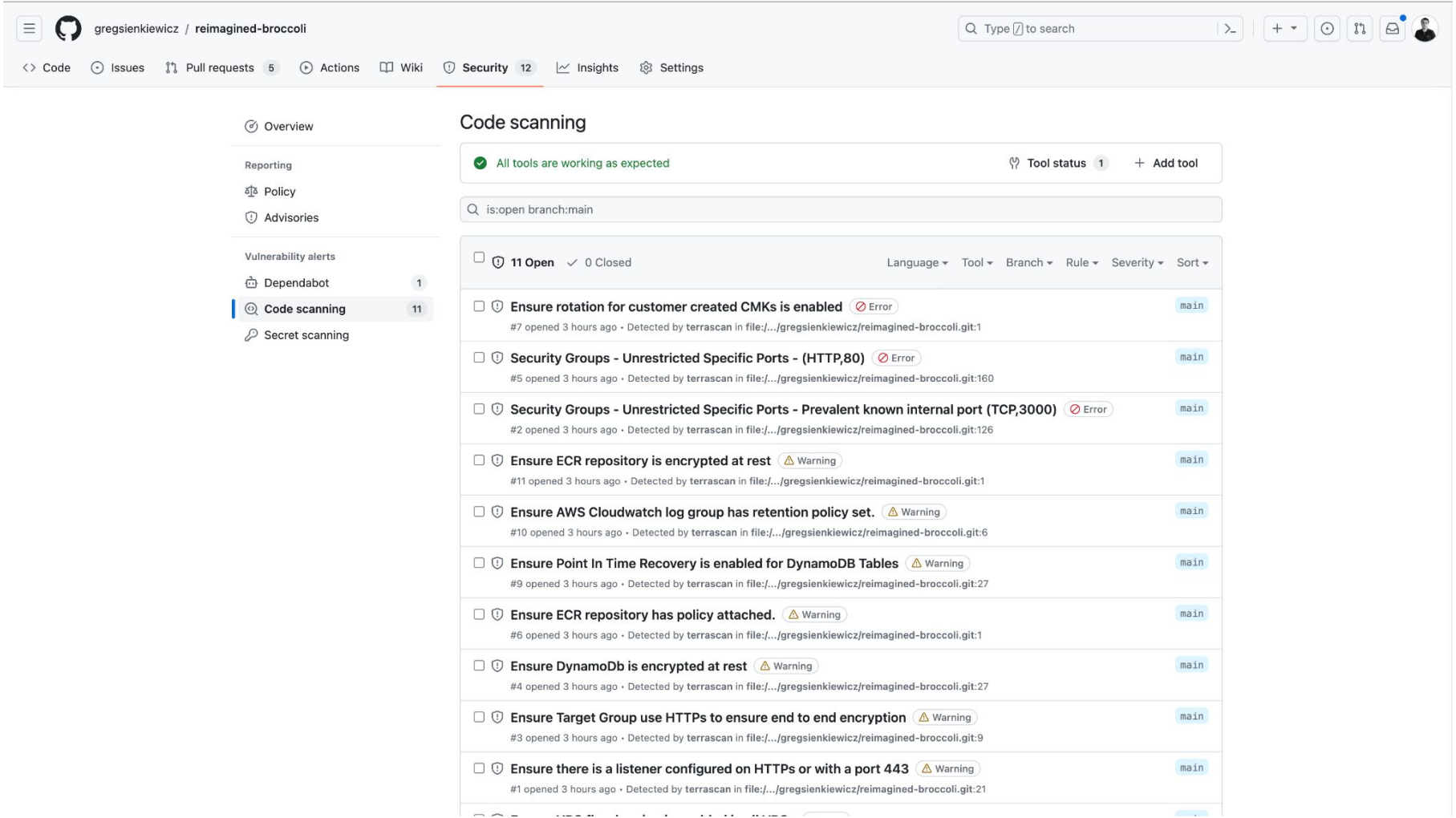
reimagined-broccoli / .github / workflows / terrascan.yml

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

Code scanning alerts / #2

Security Groups - Unrestricted Specific Ports - Prevalent known internal port (TCP,3000)

Dismiss alert Create issue

Open in main 23 minutes ago

file://https://github.com/gregsienkiewicz/**reimagined-broccoli.git**:126

Preview unavailable

Sorry, we couldn't find this file in the repository.

Security Groups - Unrestricted Specific Ports - Prevalent known internal port (TCP,3000)

terrascan

Tool	Rule ID
terrascan	AC_AWS_0264

No rule help available for this alert.

Severity

Error

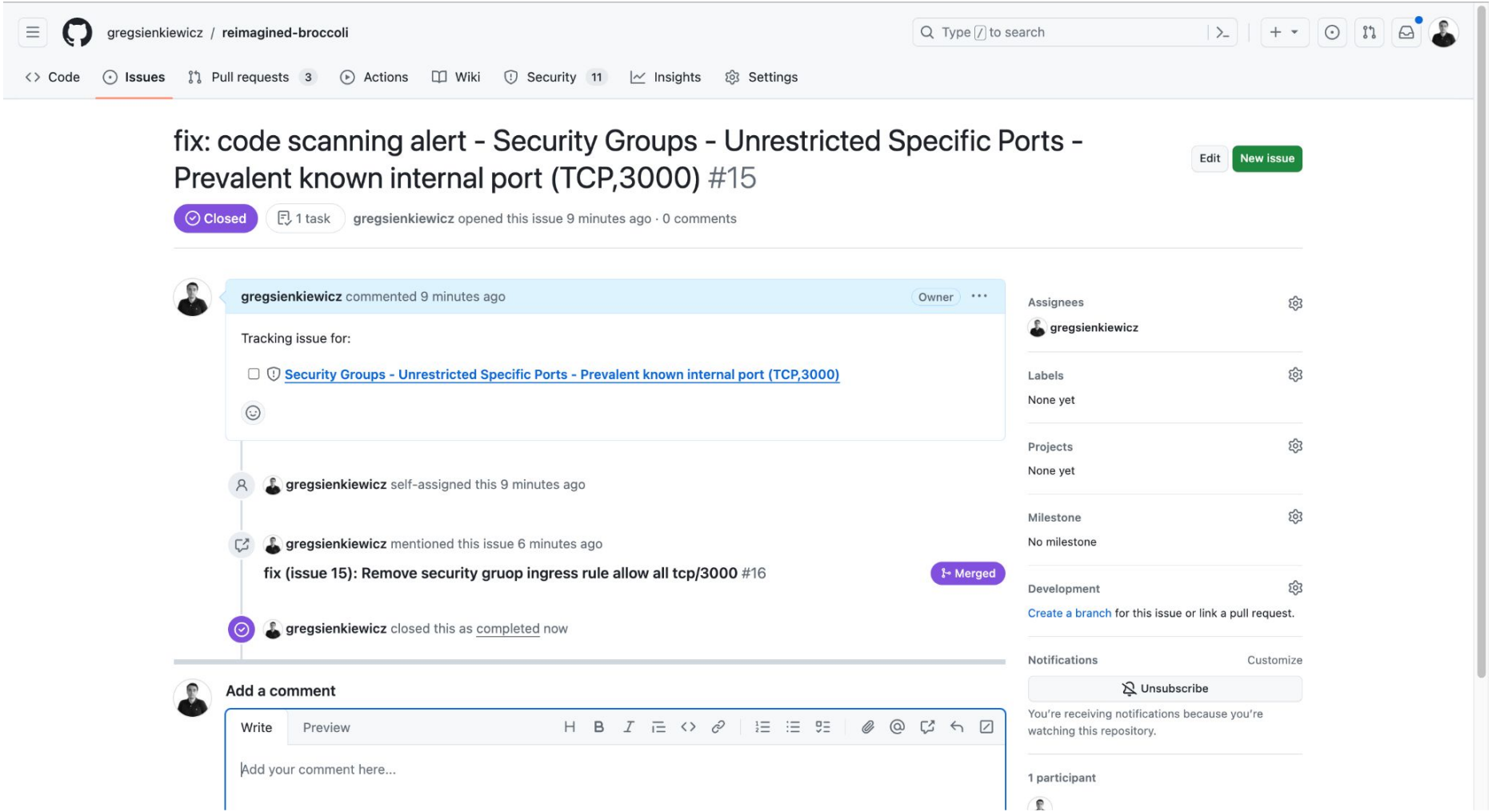
Affected branches

main

First detected in commit yesterday

Merge 92f65d2 into eb1a545 Verified 95378a7

file://https://github.com/gregsienkiewicz/**reimagined-broccoli.git:126** on branch refs/pull/6/merge


gregsienkiewicz / reimagined-broccoli
Type / to search
Code
Issues
Pull requests 3
Actions
Wiki
Security 11
Insights
Settings
fix: code scanning alert - Security Groups - Unrestricted Specific Ports - Prevalent known internal port (TCP,3000) #15
Edit
New issue
Closed
1 task
gregsienkiewicz opened this issue 9 minutes ago · 0 comments
gregsienkiewicz commented 9 minutes ago
Owner
Tracking issue for:
Security Groups - Unrestricted Specific Ports - Prevalent known internal port (TCP,3000)
gregsienkiewicz self-assigned this 9 minutes ago
gregsienkiewicz mentioned this issue 6 minutes ago
fix (issue 15): Remove security gruop ingress rule allow all tcp/3000 #16
Merged
gregsienkiewicz closed this as completed now
Add a comment
Write
Preview
Add your comment here...
Assignees
gregsienkiewicz
Labels
None yet
Projects
None yet
Milestone
No milestone
Development
Create a branch for this issue or link a pull request.
Notifications
Customize
Unsubscribe
You're receiving notifications because you're watching this repository.
1 participant

Code scanning alerts / #2

Security Groups - Unrestricted Specific Ports - Prevalent known internal port (TCP,3000)

Dismiss alert

Fixed in main now | Tracked by #15

file://https://github.com/gregsienkiewicz/**reimagined-broccoli.git**:126

Preview unavailable

Sorry, we couldn't find this file in the repository.

Security Groups - Unrestricted Specific Ports - Prevalent known internal port (TCP,3000)

terrascan

Tool	Rule ID
terrascan	AC_AWS_0264

No rule help available for this alert.

First detected in commit yesterday

Merge 92f65d2 into eb1a545 — Verified — 95378a7

file://https://github.com/gregsienkiewicz/**reimagined-broccoli.git**:126 on branch refs/pull/6/merge

Fixed in branch main now

fix (issue 15): Remove security gruop ingress rule allow all tcp/3000 (… — Verified — 980f08f

Severity

Error

Affected branches

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

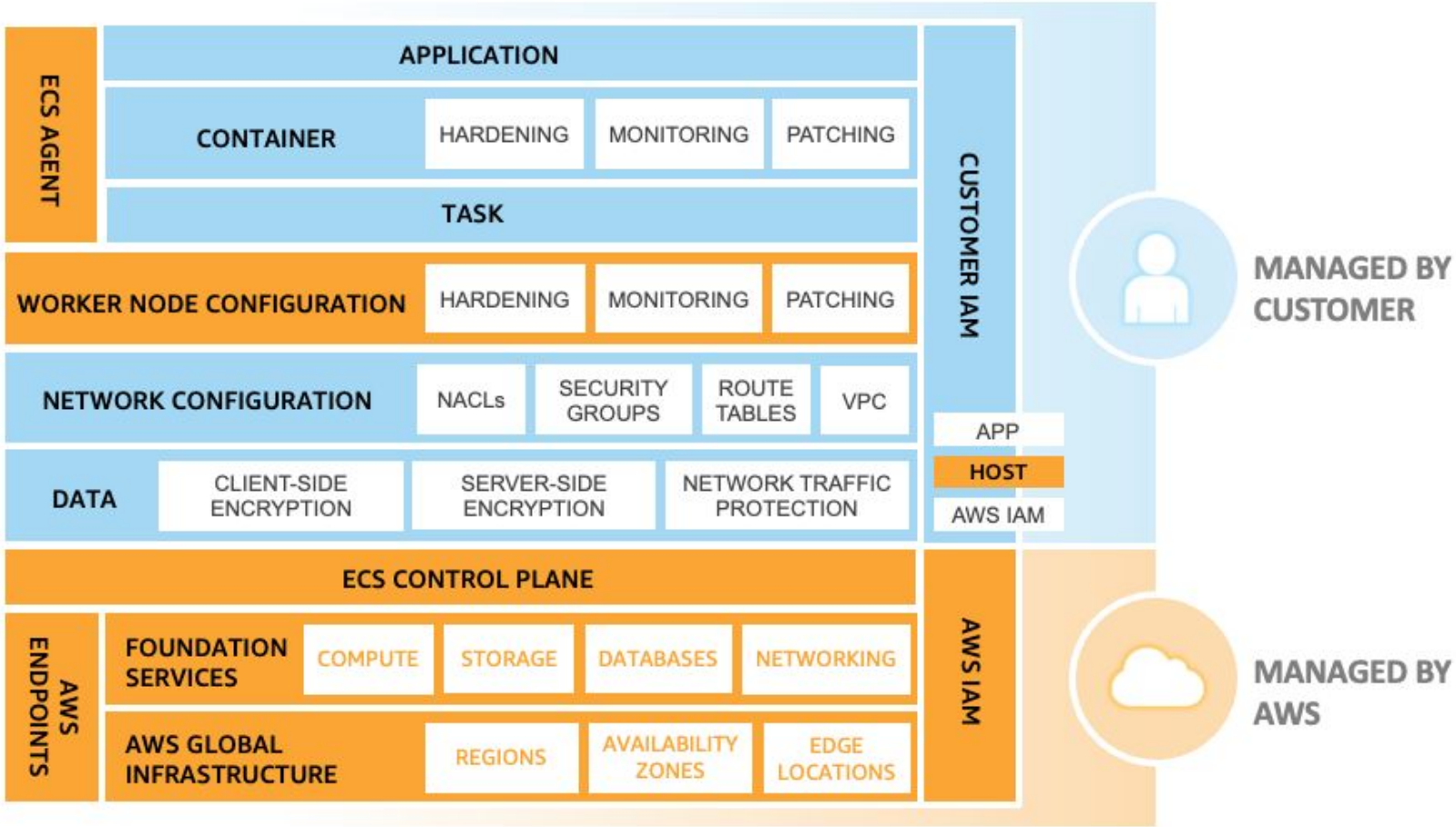
Imgbot
By imgbot
A GitHub app that optimizes your images

CodeFactor
By codefactor-io
Automated code review for GitHub

AWS

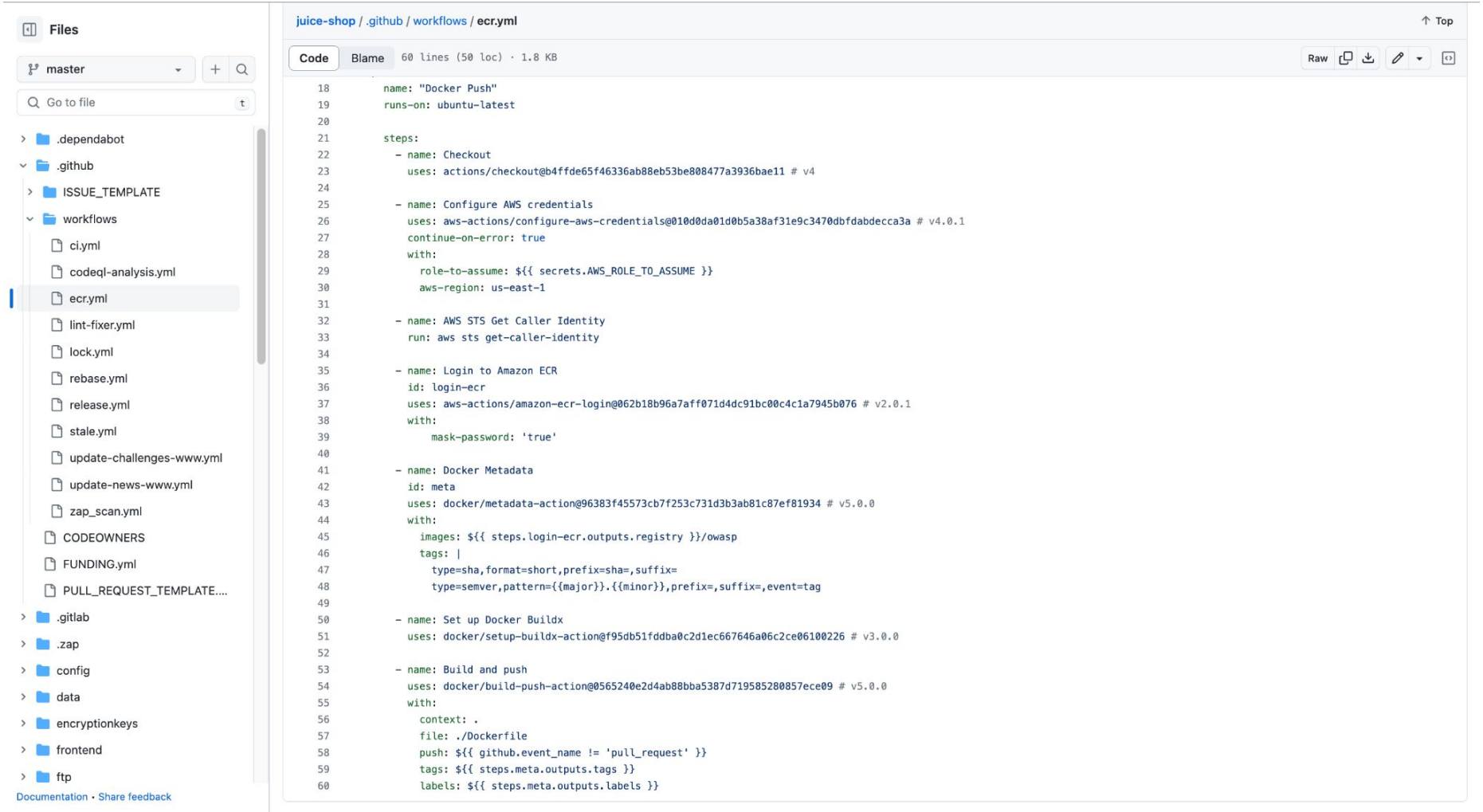
Protect the runtime.

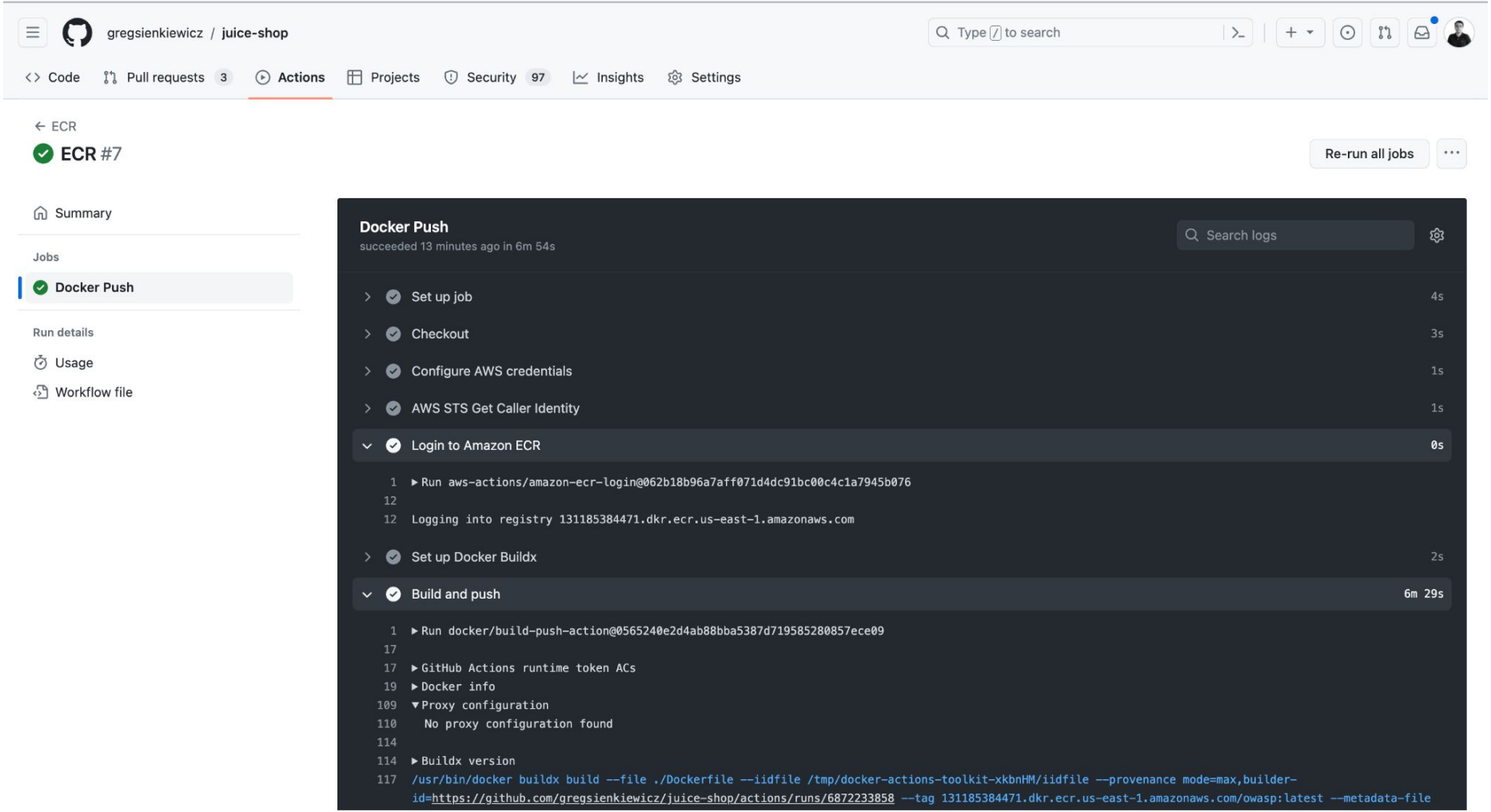
AWS Shared Responsibility Model for Amazon ECS with Fargate



Secure the ECS task and runtime

Secure your container’s images


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
.zap
config
data
encryptionkeys
frontend
ftp
Documentation
Share feedback
juice-shop / .github / workflows / ecr.yml
Top
Code
Blame
60 lines (50 loc) · 1.8 KB
Raw
name: "Docker Push"
runs-on: ubuntu-latest
steps:
- name: Checkout
uses: actions/checkout@b4ffde65f46336ab88eb53be808477a3936bae11 # v4
- name: 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: AWS STS Get Caller Identity
run: aws sts get-caller-identity
- name: Login to Amazon ECR
id: login-ecr
uses: aws-actions/amazon-ecr-login@062b18b96a7aff071d4dc91bc00c4c1a7945b076 # v2.0.1
with:
mask-password: 'true'
- name: Docker Metadata
id: meta
uses: docker/metadata-action@96383f45573cb7f253c731d3b3ab81c87ef81934 # v5.0.0
with:
images: ${{ steps.login-ecr.outputs.registry }}/owasp
tags: |
type=sha,format=short,prefix=sha=,suffix=
type=semver,pattern={{major}}.{{minor}},prefix=,suffix=,event=tag
- name: Set up Docker Buildx
uses: docker/setup-buildx-action@f95db51fddba0c2d1ec667646a06c2ce06100226 # v3.0.0
- name: Build and push
uses: docker/build-push-action@0565240e2d4ab88bba5387d719585280857ece09 # v5.0.0
with:
context: .
file: ./Dockerfile
push: ${{ github.event_name != 'pull_request' }}
tags: ${{ steps.meta.outputs.tags }}
labels: ${{ steps.meta.outputs.labels }}


gregsienkiewicz / juice-shop
Type / to search
Code
Pull requests 3
Actions
Projects
Security 97
Insights
Settings
← ECR
ECR #7
Re-run all jobs
Summary
Jobs
Docker Push
Run details
Usage
Workflow file
Docker Push
succeeded 13 minutes ago in 6m 54s
Search logs
Set up job 4s
Checkout 3s
Configure AWS credentials 1s
AWS STS Get Caller Identity 1s
Login to Amazon ECR 0s
1 ▶ Run aws-actions/amazon-ecr-login@062b18b96a7aff071d4dc91bc00c4c1a7945b076
12
12 Logging into registry 131185384471.dkr.ecr.us-east-1.amazonaws.com
Set up Docker Buildx 2s
Build and push 6m 29s
1 ▶ Run docker/build-push-action@0565240e2d4ab88bba5387d719585280857ece09
17
17 ▶ GitHub Actions runtime token ACs
19 ▶ Docker info
109 ▼ Proxy configuration
110 No proxy configuration found
114
114 ▶ Buildx version
117 /usr/bin/docker buildx build --file ./Dockerfile --iidfile /tmp/docker-actions-toolkit-xkbnHM/iidfile --provenance mode=max,builder-id=https://github.com/gregsienkiewicz/juice-shop/actions/runs/6872233858 --tag 131185384471.dkr.ecr.us-east-1.amazonaws.com/owasp:latest --metadata-file


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

Scanning configuration

Scanning configuration Info

Basic scanning is provided by default for your private registry. Enhanced scanning can be enabled for your registry to provide automated, continuous scanning to find vulnerabilities in your container images.

Scan type

Select the scanning type that will be used for this registry. Enhanced scanning has additional pricing

- ○ **Basic scanning**
  Basic scanning allows manual scans and scan on push of images in this registry. This is a free service.
- ◉ **Enhanced scanning**
  Enhanced scanning with Amazon Inspector provides automated continuous scanning. Inspector identifies vulnerabilities in both operating system and programming language (such as Python, Java, Ruby etc.) packages in real time.

Continuous scanning filters

Select which repositories will continuously have images scanned for vulnerabilities. Filters with no wildcard will match all repository names that contain the filter. Filters with wildcards (*) will match on a repository name where the wildcard replaces zero or more characters in the repository name.

☐ Continuously scan all repositories

Add filter

owasp ✕ prod ✕

Preview repository matches

Scan on push filters

Select which repositories to scan for vulnerabilities on image push. Filters with no wildcard will match all repository names that contain the filter. Filters with wildcards (*) will match on a repository name where the wildcard replaces zero or more characters in the repository name.

☑ Scan on push all repositories

Cancel Save

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

Summary

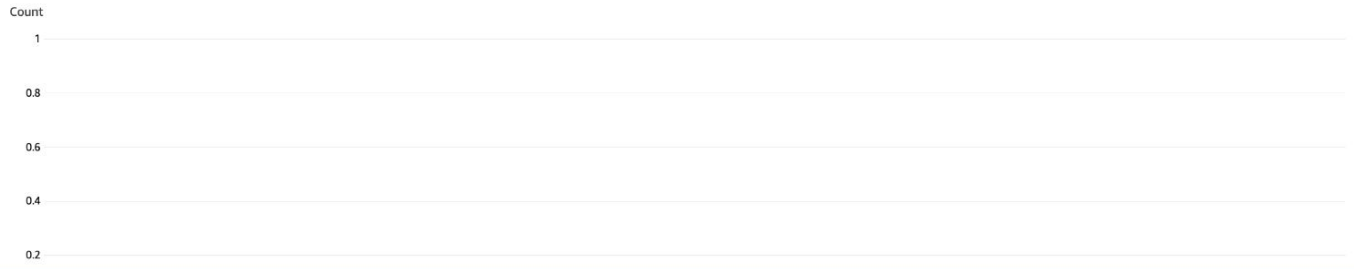
Repository details

Name owasp	Created at November 14, 2023, 21:13:39 (UTC-05)	ARN arn:aws:ecr:us-east-1:131185384471:repository/owasp
Tag immutability Immutable	Encryption type AES-256	Scan frequency Continuous
Pull through cache -		

Pull counts Info

1h 3h 12h 1d 3d 1w Custom | UTC timezone | Add to dashboard

owasp pull counts



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

Documentation • Share feedback

Code | Blame | 39 lines (33 loc) · 799 Bytes | Raw

```hcl
resource "aws_ecr_repository" "owasp" {
  name                 = "owasp"
  image_tag_mutability = "IMMUTABLE"
  force_delete         = true

  image_scanning_configuration {
    scan_on_push = true
  }
}

resource "aws_ecr_lifecycle_policy" "owasp" {
  repository = aws_ecr_repository.owasp.name

  policy = file("./ecr_lifecycle_policy.json")
}

resource "aws_ecr_registry_scanning_configuration" "test" {
  scan_type = "ENHANCED"

  rule {
    scan_frequency = "SCAN_ON_PUSH"
    repository_filter {
      filter      = "*"
      filter_type = "WILDCARD"
    }
  }

  rule {
    scan_frequency = "CONTINUOUS_SCAN"
    repository_filter {
      filter      = "owasp"
      filter_type = "WILDCARD"
    }
    repository_filter {
      filter      = "prod"
      filter_type = "WILDCARD"
    }
  }
}
```

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 / ecr_lifecycle_policy.json

gregsienkiewicz refactor: Update the ECR lifecycle policy (#14) 06f0fca · now History

Code Blame 29 lines (29 loc) · 800 Bytes Raw

```
{
    "rules": [
        {
            "rulePriority": 1,
            "description": "Keep only one untagged image, expire all others",
            "selection": {
                "tagStatus": "untagged",
                "countType": "imageCountMoreThan",
                "countNumber": 1
            },
            "action": {
                "type": "expire"
            }
        },
        {
            "rulePriority": 2,
            "description": "Keep five tagged image, expire all others",
            "selection": {
                "tagStatus": "tagged",
                "tagPrefixList": ["sha-", "v"],
                "countType": "imageCountMoreThan",
                "countNumber": 5
            },
            "action": {
                "type": "expire"
            }
        }
    ]
}
```

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

owasp

Lifecycle policy rules

Reorder | Edit | Delete | Edit test rules | Actions | Create rule

Priority	Rule description	Summary
1	Keep only one untagged image, expire all others	expire | imageCountMoreThan (1) | untagged
2	Keep five tagged image, expire all others	expire | imageCountMoreThan (5) | tagged prefix [sha-,v]

Lifecycle events history

Filter events

1

Completed at	Message
2023-11-15T16:10:07.000Z	PolicyExecutionEvent | 0 images affected

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

Amazon ECR > Repositories > owasp

owasp

View push commands | Edit

Images (8)

Delete | Details

1.0

1

Image tag	Artifact type	Pushed at	Size (MB)	Image URI	Digest	Vulnerabilities
1.0	Image Index	November 15, 2023, 11:47:44 (UTC-05)	200.85	Copy URI	sha256:e1303255eefada5…	See findings

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

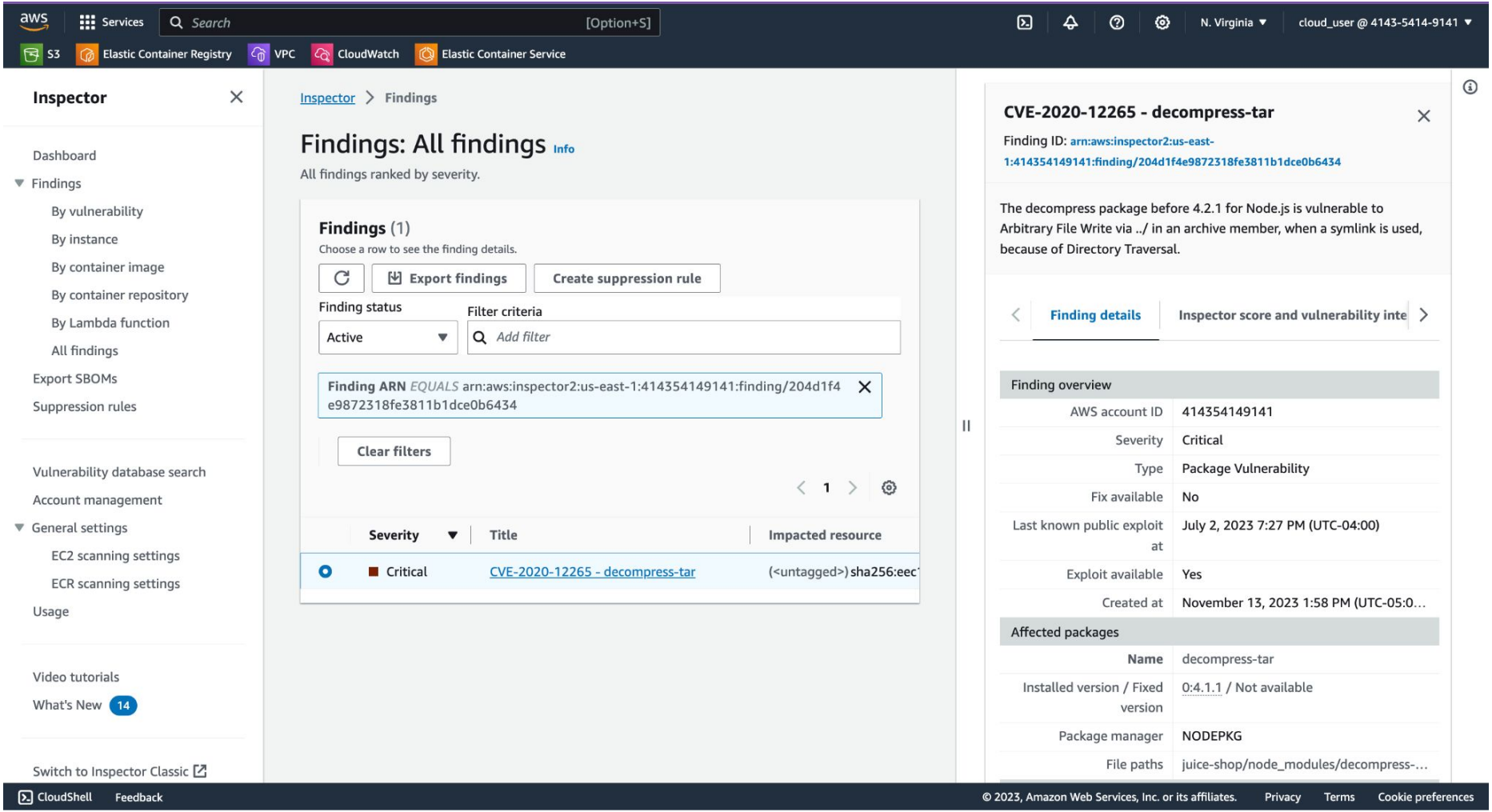
Overview

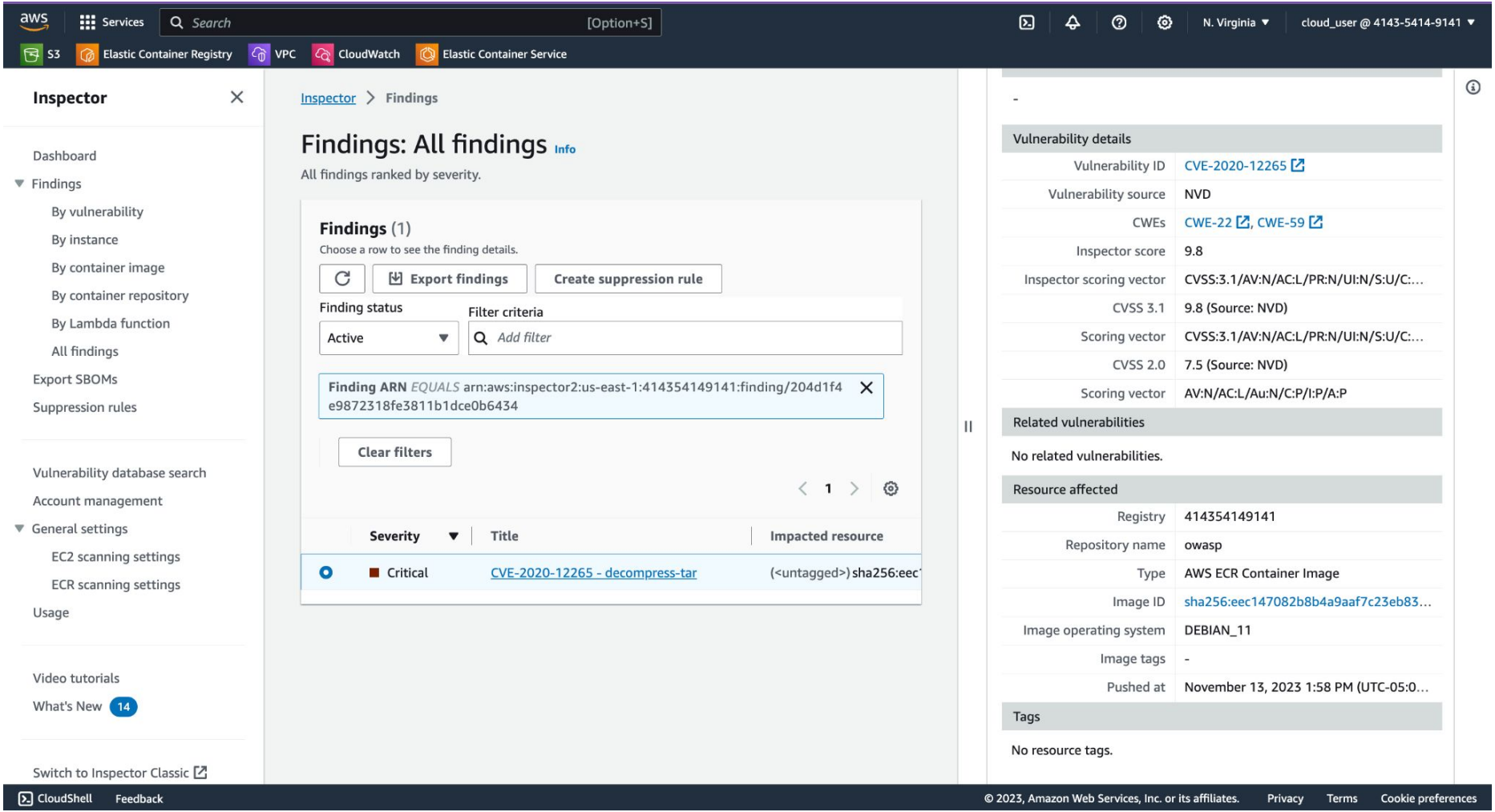
Critical	High	Medium	Low	Informational	Undefined
12	21	22	1	0	0

Vulnerabilities (56)

1

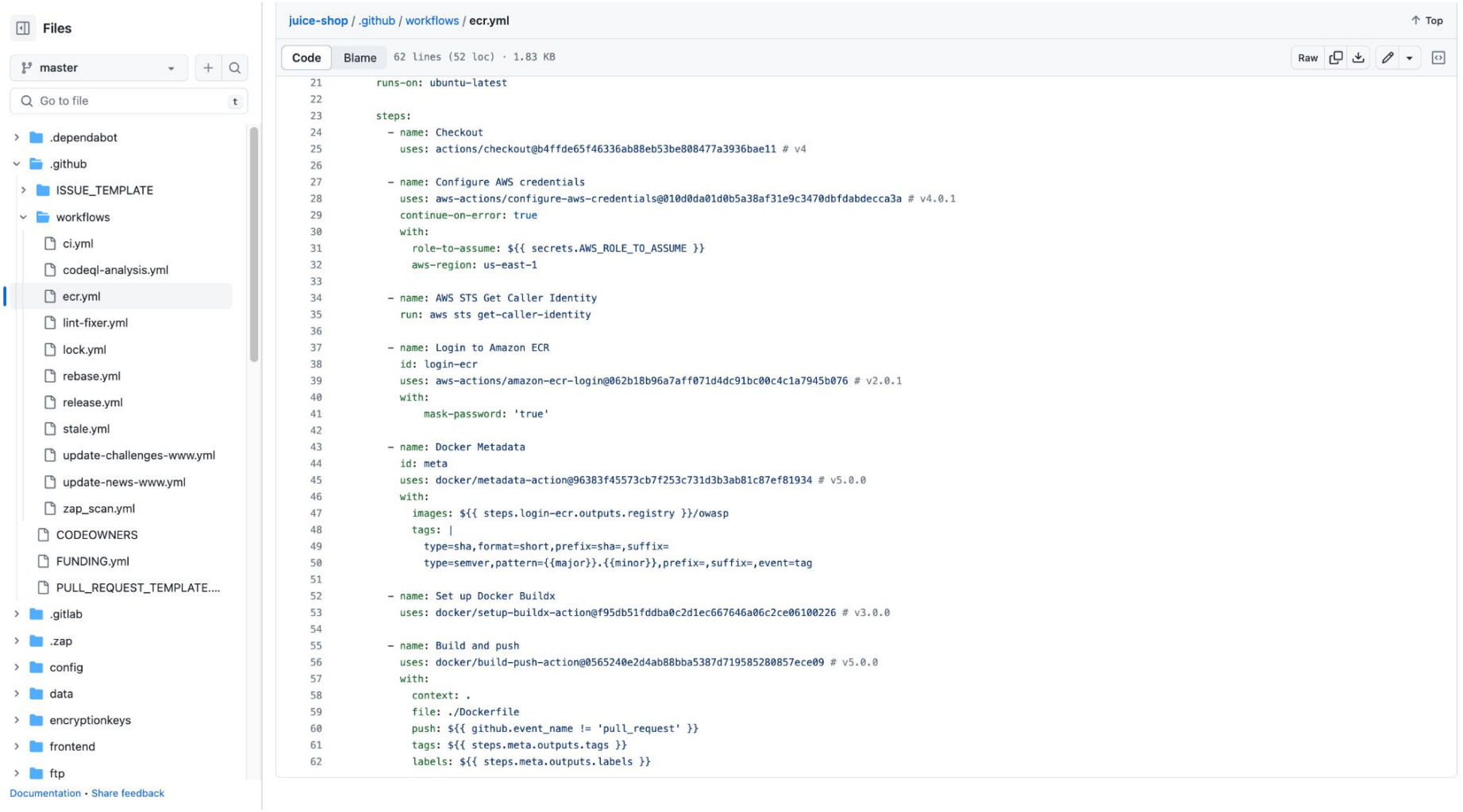
Name	Package	Severity	Description	Status	Remediation
SNYK-JS-SANITIZEHTML-585892	sanitize-html	CRITICAL	## Overview [sanitize-html](https://github.com/punkave/sanitize-html) is a library that allows you to clean up user-submitted HTML, preserving whitelisted elements and whitelisted attributes on a per-element 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


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
.zap
config
data
encryptionkeys
frontend
ftp
Documentation • Share feedback
juice-shop / .github / workflows / ecr.yml
Top
Code
Blame
62 lines (52 loc) · 1.83 KB
Raw
21 runs-on: ubuntu-latest
22
23 steps:
24 - name: Checkout
25 uses: actions/checkout@b4ffde65f46336ab88eb53be808477a3936bae11 # v4
26
27 - name: Configure AWS credentials
28 uses: aws-actions/configure-aws-credentials@010d0da01d0b5a38af31e9c3470dbfdabdecca3a # v4.0.1
29 continue-on-error: true
30 with:
31 role-to-assume: ${{ secrets.AWS_ROLE_TO_ASSUME }}
32 aws-region: us-east-1
33
34 - name: AWS STS Get Caller Identity
35 run: aws sts get-caller-identity
36
37 - name: Login to Amazon ECR
38 id: login-ecr
39 uses: aws-actions/amazon-ecr-login@062b18b96a7aff071d4dc91bc00c4c1a7945b076 # v2.0.1
40 with:
41 mask-password: 'true'
42
43 - name: Docker Metadata
44 id: meta
45 uses: docker/metadata-action@96383f45573cb7f253c731d3b3ab81c87ef81934 # v5.0.0
46 with:
47 images: ${{ steps.login-ecr.outputs.registry }}/owasp
48 tags: |
49 type=sha,format=short,prefix=sha=,suffix=
50 type=semver,pattern={{major}}.{{minor}},prefix=,suffix=,event=tag
51
52 - name: Set up Docker Buildx
53 uses: docker/setup-buildx-action@f95db51fddba0c2d1ec667646a06c2ce06100226 # v3.0.0
54
55 - name: Build and push
56 uses: docker/build-push-action@0565240e2d4ab88bba5387d719585280857ece09 # v5.0.0
57 with:
58 context: .
59 file: ./Dockerfile
60 push: ${{ github.event_name != 'pull_request' }}
61 tags: ${{ steps.meta.outputs.tags }}
62 labels: ${{ steps.meta.outputs.labels }}

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

Amazon ECR > Repositories > owasp

owasp

View push commands | Edit

Images (3)

Delete | Details

Search artifacts

1

Image tag	Artifact type	Pushed at	Size (MB)	Image URI	Digest	Vulnerabilities
sha-72b6590	Image Index	November 15, 2023, 11:40:51 (UTC-05)	200.85	Copy URI	sha256:709d8ac5939e49…	See findings
-	Image	November 15, 2023, 11:40:50 (UTC-05)	0.04	Copy URI	sha256:0c7c78b1a6098f6…	See findings
-	Image	November 15, 2023, 11:40:50 (UTC-05)	200.85	Copy URI	sha256:6424d52a09d3c1…	See findings

Summary

Jobs

Docker Push

Run details

Usage

Workflow file

Docker Push

failed 1 minute ago in 5m 35s

Search logs

Build and push 5m 12s

```
#33 exporting attestation manifest sha256:c5e916bd75fdae3580fe3b89808a225f83b88c2808c7f1b58a9bcf1d5ef94352
#33 ...

#34 [auth] sharing credentials for 040546586270.dkr.ecr.us-east-1.amazonaws.com
#34 DONE 0.0s

#33 exporting to image
#33 exporting attestation manifest sha256:c5e916bd75fdae3580fe3b89808a225f83b88c2808c7f1b58a9bcf1d5ef94352 done
#33 exporting manifest list sha256:e1303255eefada56e3c3f2bf51e49928e19e033e807fcd1247cc4727ae375c22 done
#33 pushing layers
#33 pushing layers 8.2s done
#33 pushing manifest for 040546586270.dkr.ecr.us-east-1.amazonaws.com/owasp:1.0@sha256:e1303255eefada56e3c3f2bf51e49928e19e033e807fcd1247cc4727ae375c22
#33 pushing manifest for 040546586270.dkr.ecr.us-east-1.amazonaws.com/owasp:1.0@sha256:e1303255eefada56e3c3f2bf51e49928e19e033e807fcd1247cc4727ae375c22 0.9s done
#33 pushing layers 0.3s done
#33 pushing manifest for 040546586270.dkr.ecr.us-east-1.amazonaws.com/owasp:sha-72b6590@sha256:e1303255eefada56e3c3f2bf51e49928e19e033e807fcd1247cc4727ae375c22
#33 pushing manifest for 040546586270.dkr.ecr.us-east-1.amazonaws.com/owasp:sha-72b6590@sha256:e1303255eefada56e3c3f2bf51e49928e19e033e807fcd1247cc4727ae375c22 0.4s done
#33 ERROR: failed to push 040546586270.dkr.ecr.us-east-1.amazonaws.com/owasp:sha-72b6590: failed commit on ref "index-
sha256:e1303255eefada56e3c3f2bf51e49928e19e033e807fcd1247cc4727ae375c22": unexpected status from PUT request to https://040546586270.dkr.ecr.us-east-
1.amazonaws.com/v2/owasp/manifests/sha-72b6590: 400 Bad Request
------
 > exporting to image:
------
ERROR: failed to solve: failed to push 040546586270.dkr.ecr.us-east-1.amazonaws.com/owasp:sha-72b6590: failed commit on ref "index-
sha256:e1303255eefada56e3c3f2bf51e49928e19e033e807fcd1247cc4727ae375c22": unexpected status from PUT request to https://040546586270.dkr.ecr.us-east-
1.amazonaws.com/v2/owasp/manifests/sha-72b6590: 400 Bad Request
Error: buildx failed with: ERROR: failed to solve: failed to push 040546586270.dkr.ecr.us-east-1.amazonaws.com/owasp:sha-72b6590: failed commit on ref "index-
sha256:e1303255eefada56e3c3f2bf51e49928e19e033e807fcd1247cc4727ae375c22": unexpected status from PUT request to https://040546586270.dkr.ecr.us-east-
1.amazonaws.com/v2/owasp/manifests/sha-72b6590: 400 Bad Request
```

Post Build and push 0s

Post Set up Docker Buildx 11s

Post Login to Amazon ECR 0s

Post Configure AWS credentials 0s

Post Checkout 0s

Complete job 0s

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

Amazon ECR > Repositories > owasp

owasp

View push commands | Edit

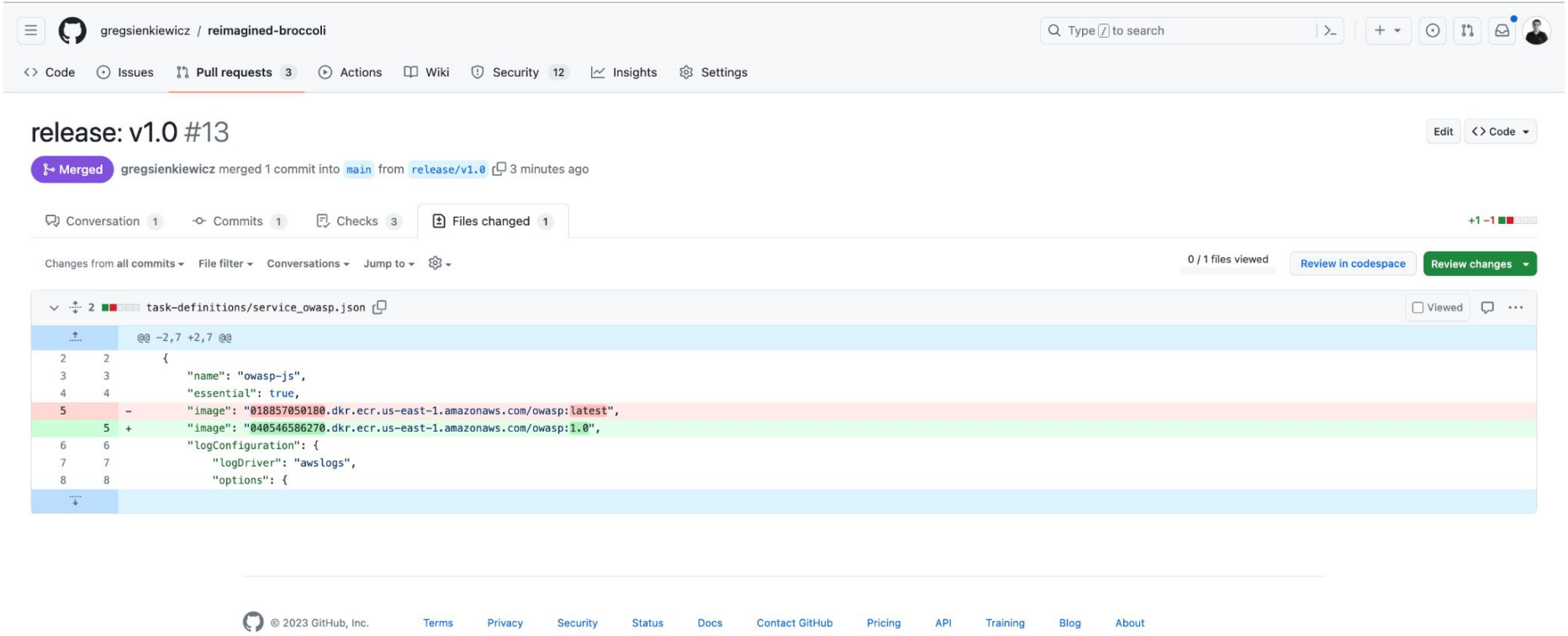
Images (8)

Delete | Details

1.0

1

Image tag	Artifact type	Pushed at	Size (MB)	Image URI	Digest	Vulnerabilities
1.0	Image Index	November 15, 2023, 11:47:44 (UTC-05)	200.85	Copy URI	sha256:e1303255eefada5…	See findings


gregsienkiewicz / reimagined-broccoli
Type / to search
Code
Issues
Pull requests 3
Actions
Wiki
Security 12
Insights
Settings
release: v1.0 #13
Edit
Code
Merged
gregsienkiewicz merged 1 commit into main from release/v1.0 3 minutes ago
Conversation 1
Commits 1
Checks 3
Files changed 1
+1 −1
Changes from all commits
File filter
Conversations
Jump to
0 / 1 files viewed
Review in codespace
Review changes
2 task-definitions/service_owasp.json
Viewed
@@ -2,7 +2,7 @@
{
"name": "owasp-js",
"essential": true,
- "image": "018857050180.dkr.ecr.us-east-1.amazonaws.com/owasp:latest",
+ "image": "040546586270.dkr.ecr.us-east-1.amazonaws.com/owasp:1.0",
"logConfiguration": {
"logDriver": "awslogs",
"options": {
© 2023 GitHub, Inc.
Terms
Privacy
Security
Status
Docs
Contact GitHub
Pricing
API
Training
Blog
About

Summary

Jobs

Apply (backend, tfvars/backen...

Run details

Usage

Workflow file

Apply (backend, tfvars/backend.tfvars)

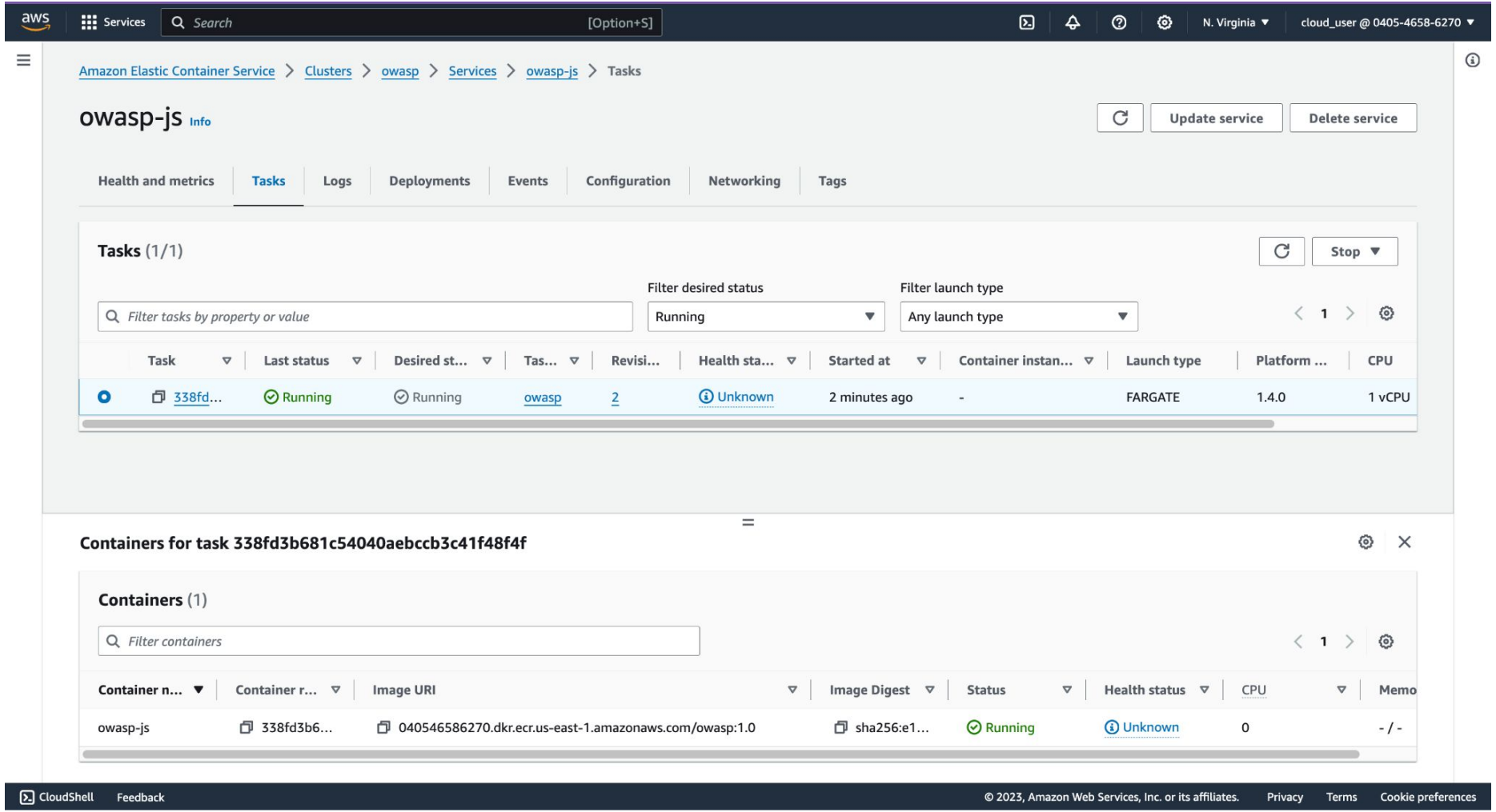
succeeded 1 minute ago in 1m 40s

Search logs

Terraform Apply 9s

```
-/+ destroy and then create replacement

Terraform will perform the following actions:

  # aws_ecs_service.owasp will be updated in-place
  ~ resource "aws_ecs_service" "owasp" {
        id                                 = "arn:aws:ecs:us-east-1:040546586270:service/owasp/owasp-js"
        name                               = "owasp-js"
        tags                               = {}
      ~ task_definition                    = "arn:aws:ecs:us-east-1:040546586270:task-definition/owasp:1" -> (known after apply)
        # (15 unchanged attributes hidden)

        # (4 unchanged blocks hidden)
    }

  # aws_ecs_task_definition.owasp must be replaced
-/+ resource "aws_ecs_task_definition" "owasp" {
      ~ arn                    = "arn:aws:ecs:us-east-1:040546586270:task-definition/owasp:1" -> (known after apply)
      ~ arn_without_revision   = "arn:aws:ecs:us-east-1:040546586270:task-definition/owasp" -> (known after apply)
      ~ container_definitions  = jsonencode(
          ~ [
              ~ {
                  - cpu             = 0
                  - environment     = []
                  ~ image           = "018857050180.dkr.ecr.us-east-1.amazonaws.com/owasp:latest" -> "040546586270.dkr.ecr.us-east-1.amazonaws.com/owasp:1.0"
                  - mountPoints     = []
                    name            = "owasp-js"
                  - volumesFrom     = []
                    # (4 unchanged attributes hidden)
                },
            ] # forces replacement
        )
      ~ id                     = "owasp" -> (known after apply)
      ~ revision               = 1 -> (known after apply)
      - tags                   = {} -> null
        # (8 unchanged attributes hidden)

        # (1 unchanged block hidden)
    }

  # aws_route_table.private will be updated in-place
```

https://github.com/gregsienkiewicz/reimagined-broccoli/actions/runs/6880587688/job/18715122584#step:10:81


aws
Services
Search
[Option+S]
N. Virginia
cloud_user @ 0405-4658-6270
Amazon Elastic Container Service > Clusters > owasp > Services > owasp-js > Tasks
owasp-js Info
Update service
Delete service
Health and metrics
Tasks
Logs
Deployments
Events
Configuration
Networking
Tags
Tasks (1/1)
Stop
Filter desired status
Running
Filter launch type
Any launch type
Filter tasks by property or value
Task
Last status
Desired st...
Tas...
Revisi...
Health sta...
Started at
Container instan...
Launch type
Platform ...
CPU
338fd...
Running
Running
owasp
2
Unknown
2 minutes ago
-
FARGATE
1.4.0
1 vCPU
Containers for task 338fd3b681c54040aebccb3c41f48f4f
Containers (1)
Filter containers
Container n...
Container r...
Image URI
Image Digest
Status
Health status
CPU
Memo
owasp-js
338fd3b6...
040546586270.dkr.ecr.us-east-1.amazonaws.com/owasp:1.0
sha256:e1...
Running
Unknown
0
- / -
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Secure the ECS task and runtime

Secure your containers and tasks

10 best practices to containerize Node.js web applications with Docker

01 Use officially supported and deterministic image tags

- Avoid `FROM node`
- Avoid `FROM node:lts`
- Avoid `FROM node:14-alpine`

Avoid Alpine which isn't officially supported. Avoid other image tags which have a high software footprint. Prefer a slimmer, up-to-date and LTS version:

- `FROM node:16.17.0-bullseye-slim`

02 Install only production dependencies

Avoid pulling devDependencies and non-deterministic package install like the ones below:

- Avoid `RUN npm install`
- Avoid `RUN yarn install`
- Avoid `RUN npm ci`

Instead, ensure you are installing only production dependencies in a reproducible way:

- `RUN npm ci --only=production`

03 Optimize Node.js apps for production

Some Node.js libraries and frameworks will only enable production-related optimization if they detect that the NODE_ENV env var set to production:

- `ENV NODE_ENV production`

04 Don't run Node.js apps as root

Docker defaults to running the process in the container as the root user, which is a precarious security practice. Use a low privileged user and proper filesystem permissions:

- `USER node`
- `COPY --chown=node:node . /usr/src/app`

05 Properly handle events to safely terminate a Node.js application

Docker creates processes as PID 1, and they must inherently handle process signals to function properly. This is why you should avoid any of these variations:

- `CMD "npm" "start"`
- `CMD ["yarn", "start"]`
- `CMD "node" "server.js"`
- `CMD "start-app.sh"`

Instead, use a lightweight init system, such as **dumb-init**, to properly spawn the Node.js runtime process with signals support:

- `CMD ["dumb-init", "node", "server.js"]`

06 Gracefully tear down Node.js apps

Avoid an abrupt termination of a running Node.js application that halts live connections. Instead, use a process signal event handler:

```
async function closeGracefully(signal) {
   await fastify.close()
   process.kill(process.pid, signal);
}
process.on('SIGINT', closeGracefully)
```

07 Find and fix security vulnerabilities in your Node.js Docker image

Docker base images may include security vulnerabilities in the software toolchain they bundle, including the Node.js runtime itself. Scan and fix security vulnerabilities with the free Snyk Container tool which also provides base image recommendations:

- `npm install -g snyk`
- `snyk auth`
- `snyk container test node:16.17.0-bullseye-slim --file=Dockerfile`

08 Use multi-stage builds

Avoid having one big build stage when attempting to clean up sensitive data from it or dangling dependencies. Instead, use multi-stage Docker image builds and separate concerns between the build flow and the creation of a production base image.

09 Use .dockerignore

Use **.dockerignore** to ensure:

- local artifacts of node_modules/ aren't copied into the container image.
- sensitive files, such as **.npmrc**, **.env** or others, aren't leaked into the container image.
- a small Docker base image without redundant and unnecessary files.

10 Mount secrets into the Docker image

Secrets are a tricky thing to manage. Avoid the following security pitfalls:

- passing secrets via build arguments in non multi-stage builds
- putting secrets inside the Dockerfile

Instead, use the built-in secrets mounting. To mount a **.npmrc** file for package install:

- In the Dockerfile: `RUN --mount=type=secret,id=npmrc, target=/usr/src/app/.npmrc npm ci --only=production`
- Then build the image with: `docker build . --build-arg NPM_TOKEN=1234 --secret id=npmrc,src=.npmrc`

Authors
@liran_tal
@goldbergyoni

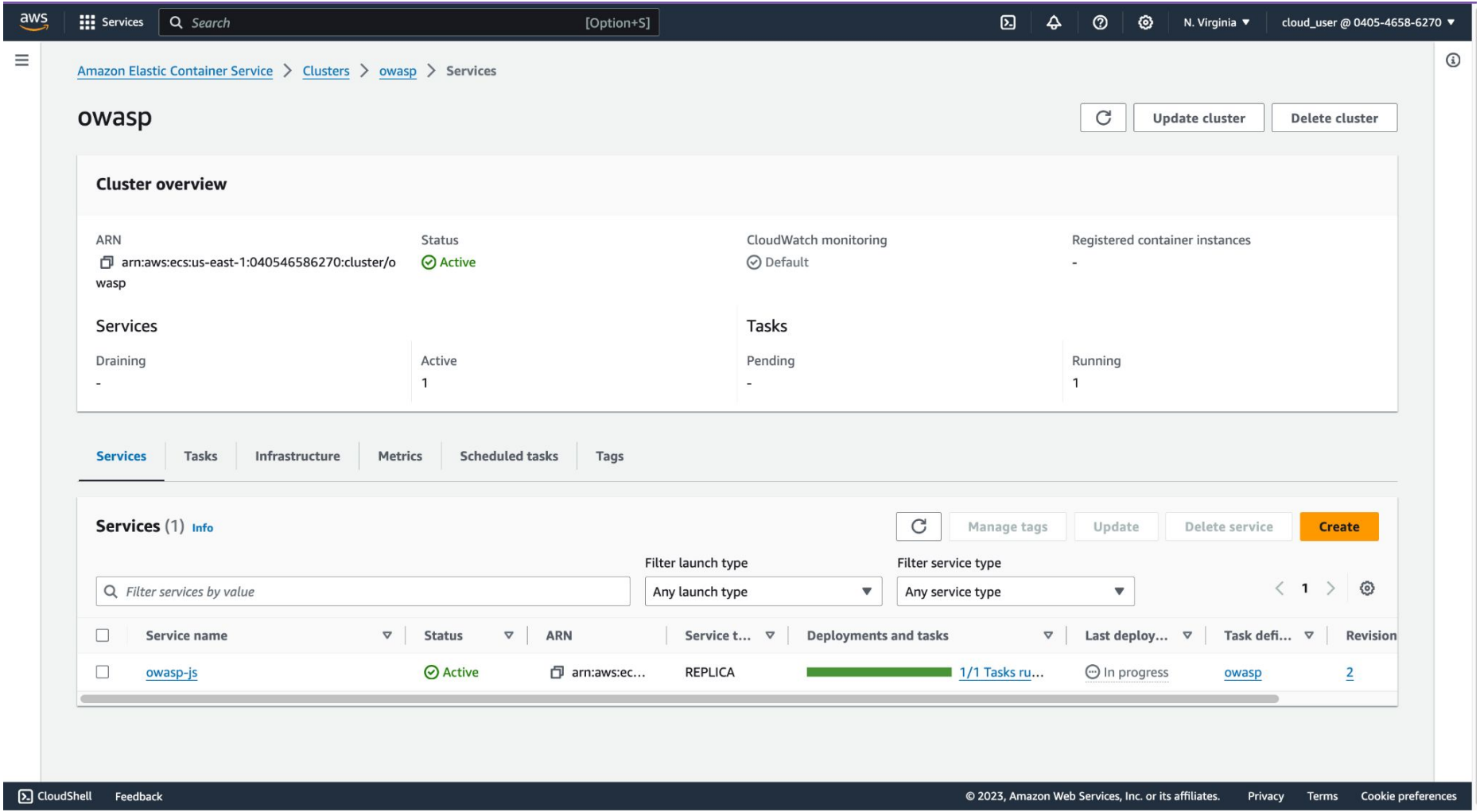
snyk

```
FROM node:18-buster as installer
COPY . /juice-shop
WORKDIR /juice-shop
RUN npm i -g typescript ts-node
RUN npm install --omit=dev --unsafe-perm
RUN npm dedupe
RUN rm -rf frontend/node_modules
RUN rm -rf frontend/.angular
RUN rm -rf frontend/src/assets
RUN mkdir logs
RUN chown -R 65532 logs
RUN chgrp -R 0 ftp/ frontend/dist/ logs/ data/ i18n/
RUN chmod -R g=u ftp/ frontend/dist/ logs/ data/ i18n/
RUN rm data/chatbot/botDefaultTrainingData.json || true
RUN rm ftp/legal.md || true
RUN rm i18n/*.json || true

ARG CYCLONEDX_NPM_VERSION=latest
RUN npm install -g @cyclonedx/cyclonedx-npm@$CYCLONEDX_NPM_VERSION
RUN npm run sbom

# workaround for libxmljs startup error
FROM node:18-buster as libxmljs-builder
WORKDIR /juice-shop
RUN apt-get update && apt-get install -y build-essential python3
COPY --from=installer /juice-shop/node_modules ./node_modules
RUN rm -rf node_modules/libxmljs2/build && \
  cd node_modules/libxmljs2 && \
  npm run build

FROM gcr.io/distroless/nodejs18-debian11
ARG BUILD_DATE
ARG VCS_REF
LABEL maintainer="Bjoern Kimminich <bjoern.kimminich@owasp.org>" \
    org.opencontainers.image.title="OWASP Juice Shop" \
    org.opencontainers.image.description="Probably the most modern and sophisticated insecure web application" \
    org.opencontainers.image.authors="Bjoern Kimminich <bjoern.kimminich@owasp.org>" \
    org.opencontainers.image.vendor="Open Web Application Security Project" \
    org.opencontainers.image.documentation="https://help.owasp-juice.shop" \
    org.opencontainers.image.licenses="MIT" \
    org.opencontainers.image.version="15.3.0" \
    org.opencontainers.image.url="https://owasp-juice.shop" \
    org.opencontainers.image.source="https://github.com/gregsienkiewicz/juice-shop" \
    org.opencontainers.image.revision=$VCS_REF \
    org.opencontainers.image.created=$BUILD_DATE
WORKDIR /juice-shop
COPY --from=installer --chown=65532:0 /juice-shop .
COPY --chown=65532:0 --from=libxmljs-builder /juice-shop/node_modules/libxmljs2 ./node_modules/libxmljs2
USER 65532
EXPOSE 3000
CMD ["/juice-shop/build/app.js"]
```

Secure your ECS deployment

Security Best Practices, Laundry List

- Network segmentation and isolation
- Use network encryption where applicable
- Create clusters in separate VPCs when network traffic needs to be strictly isolated
- Configure AWS PrivateLink endpoints when possible
- Create automated pipelines
- Enforce least privilege when setting up policies for Amazon ECS resources
- Specify your task’s role
- Audit Amazon ECS API access
- **Use Secrets Manager or Amazon EC2 Systems Manager Parameter Store for storing secret materials**


aws
Services
Search
[Option+S]
N. Virginia
cloud_user @ 0405-4658-6270
Amazon Elastic Container Service
Clusters
owasp
Services
owasp
Update cluster
Delete cluster
Cluster overview
ARN
arn:aws:ecs:us-east-1:040546586270:cluster/owasp
Status
Active
CloudWatch monitoring
Default
Registered container instances
-
Services
Draining
-
Active
1
Tasks
Pending
-
Running
1
Services
Tasks
Infrastructure
Metrics
Scheduled tasks
Tags
Services (1) Info
Manage tags
Update
Delete service
Create
Filter services by value
Filter launch type
Any launch type
Filter service type
Any service type
1
Service name
Status
ARN
Service t...
Deployments and tasks
Last deploy...
Task defi...
Revision
owasp-js
Active
arn:aws:ec...
REPLICA
1/1 Tasks ru...
In progress
owasp
2
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

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

Documentation • Share feedback

gregsienkiewicz feature: Add AWS resources (#4) ✓ eb1a545 · 3 days ago History

Code Blame 49 lines (42 loc) · 1.29 KB Raw

```
resource "aws_ecs_cluster" "owasp" {
  name = "owasp"

  configuration {
    execute_command_configuration {
      kms_key_id = aws_kms_key.owasp.arn
      logging    = "OVERRIDE"

      log_configuration {
        cloud_watch_encryption_enabled = true
        cloud_watch_log_group_name     = aws_cloudwatch_log_group.owasp.name
      }
    }
  }
}

resource "aws_ecs_service" "owasp" {
  name            = "owasp-js"
  launch_type     = "FARGATE"
  cluster         = aws_ecs_cluster.owasp.id
  task_definition = aws_ecs_task_definition.owasp.arn
  desired_count   = 1

  network_configuration {
    subnets         = [aws_subnet.private_a.id, aws_subnet.private_b.id]
    security_groups = [aws_security_group.ecs.id]
  }

  load_balancer {
    target_group_arn = aws_lb_target_group.owasp.arn
    container_name   = "owasp-js"
    container_port   = 3000
  }
}

resource "aws_ecs_task_definition" "owasp" {
  family                   = "owasp"
  requires_compatibilities = ["FARGATE"]
  network_mode             = "awsvpc"
  cpu                      = 1024
  memory                   = 2048
  execution_role_arn       = aws_iam_role.ecs.arn
  container_definitions    = file("task-definitions/service_owasp.json")
```

owasp-js Info

Update service | Delete service

Health and metrics | Tasks | Logs | Deployments | Events | Configuration | Networking | Tags

Status Info

ARN
arn:aws:ecs:us-east-1:040546586270:service/owasp/owasp-js

Status
Active

Tasks (1 Desired)
0 Pending | 1 Running

Deployments current state
7 Failed 1 Completed

Health check grace period
0 seconds

▼ Load balancer health

(Application Load Balancer) owasp-lb

View load balancer

Listener protocol:port	Target group name:protocol	Health check path	Targets (2 total)
HTTP:80	tg-owasp-lb-ip:HTTP	/	1 Healthy 0 Unhealthy

Health

Alarm recommendations

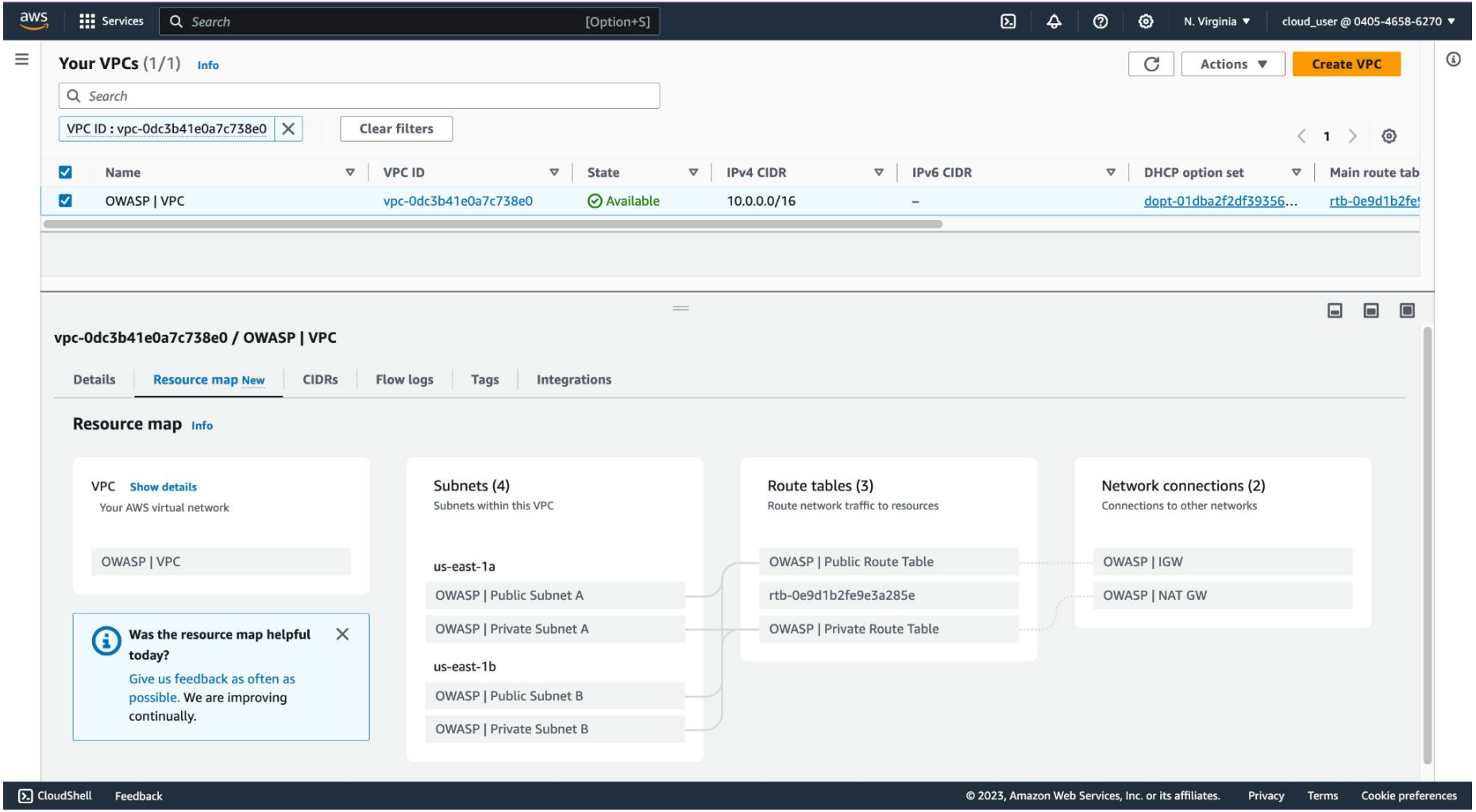
1h 3h 12h 1d 3d 1w Custom UTC timezone Add to dashboard

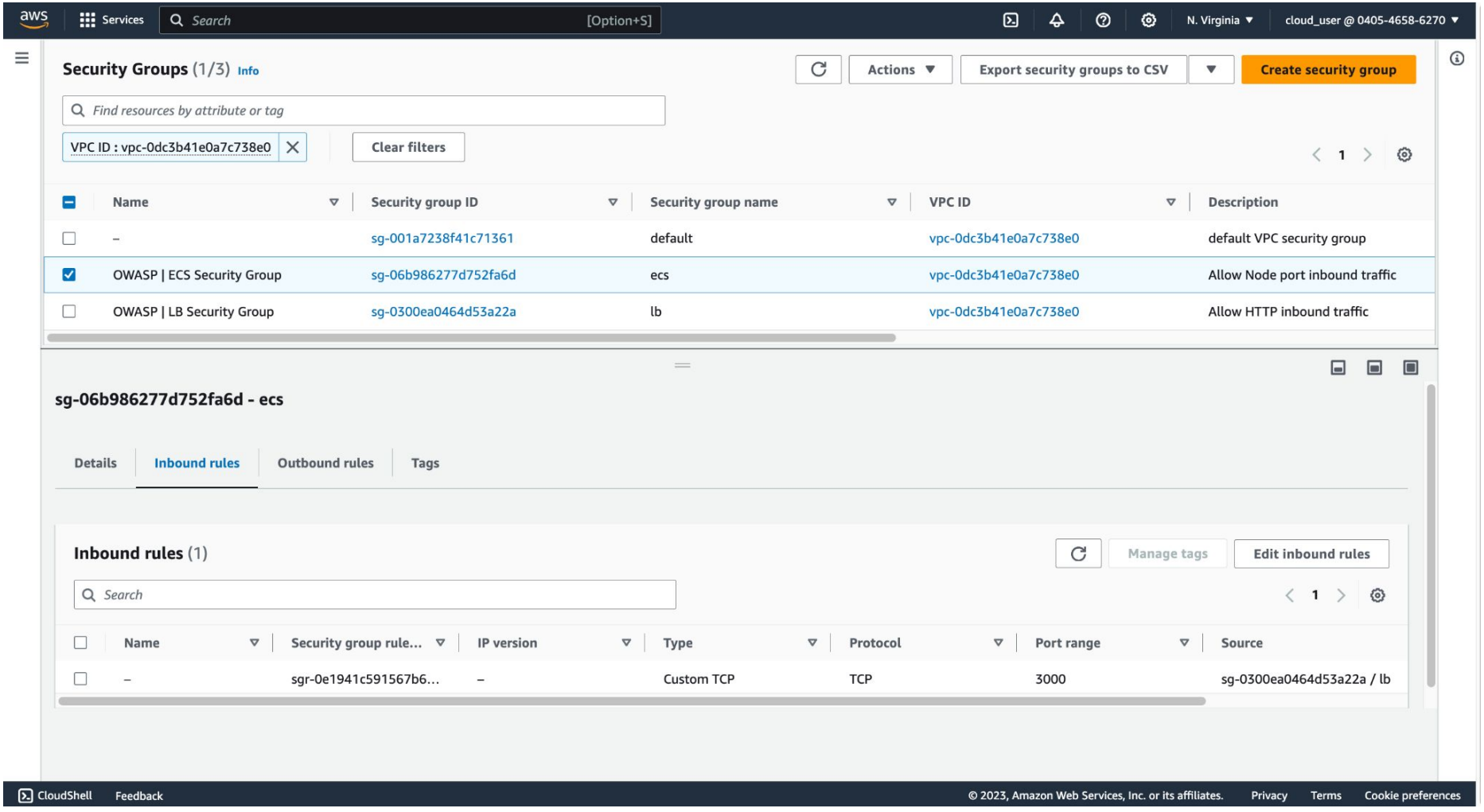
CPU utilization

Percent

Memory utilization

Percent


aws
Services
Search
[Option+S]
N. Virginia
cloud_user @ 0405-4658-6270
Your VPCs (1/1) Info
Actions
Create VPC
Search
VPC ID : vpc-0dc3b41e0a7c738e0
Clear filters
1
Name
VPC ID
State
IPv4 CIDR
IPv6 CIDR
DHCP option set
Main route tab
OWASP | VPC
vpc-0dc3b41e0a7c738e0
Available
10.0.0.0/16
–
dopt-01dba2f2df39356...
rtb-0e9d1b2fe
vpc-0dc3b41e0a7c738e0 / OWASP | VPC
Details
Resource map New
CIDRs
Flow logs
Tags
Integrations
Resource map Info
VPC Show details
Your AWS virtual network
OWASP | VPC
Was the resource map helpful today?
Give us feedback as often as possible. We are improving continually.
Subnets (4)
Subnets within this VPC
us-east-1a
OWASP | Public Subnet A
OWASP | Private Subnet A
us-east-1b
OWASP | Public Subnet B
OWASP | Private Subnet B
Route tables (3)
Route network traffic to resources
OWASP | Public Route Table
rtb-0e9d1b2fe9e3a285e
OWASP | Private Route Table
Network connections (2)
Connections to other networks
OWASP | IGW
OWASP | NAT GW
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Option+S]
N. Virginia
cloud_user @ 0405-4658-6270
Security Groups (1/3) Info
Actions
Export security groups to CSV
Create security group
Find resources by attribute or tag
VPC ID : vpc-0dc3b41e0a7c738e0
Clear filters
1
Name
Security group ID
Security group name
VPC ID
Description
– sg-001a7238f41c71361 default vpc-0dc3b41e0a7c738e0 default VPC security group
OWASP | ECS Security Group sg-06b986277d752fa6d ecs vpc-0dc3b41e0a7c738e0 Allow Node port inbound traffic
OWASP | LB Security Group sg-0300ea0464d53a22a lb vpc-0dc3b41e0a7c738e0 Allow HTTP inbound traffic
sg-06b986277d752fa6d - ecs
Details
Inbound rules
Outbound rules
Tags
Inbound rules (1)
Manage tags
Edit inbound rules
Search
1
Name
Security group rule...
IP version
Type
Protocol
Port range
Source
– sgr-0e1941c591567b6... – Custom TCP TCP 3000 sg-0300ea0464d53a22a / lb
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

owasp-js Info

Update service | Delete service

Health and metrics | Tasks | Logs | Deployments | Events | Configuration | Networking | Tags

Network configuration

Network
vpc-0dc3b41e0a7c738e0

Subnets
subnet-02a09b5c295589a88
subnet-0fa684024474b90e5

Security groups
sg-06b986277d752fa6d

Auto-assign public IP
Turned off

Health check grace period
-

Service role
AWSServiceRoleForECS

Load balancers
owasp-lb

DNS names
owasp-lb-1497288556.us-east-1.elb.amazonaws.com | open address

Target groups
tg-owasp-lb-ip

Not Secure | owasp-lb-1497288556.us-east-1.elb.amazonaws.com/#/

OWASP Juice Shop

Account EN

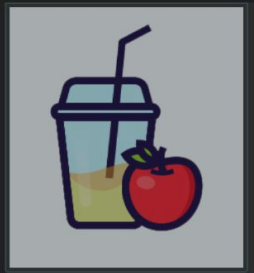
Welcome to OWASP Juice Shop!

Being a web application with a vast number of intended security vulnerabilities, the ***OWASP Juice Shop*** is supposed to be the opposite of a best practice or template application for web developers: It is an awareness, training, demonstration and exercise tool for security risks in modern web applications. The ***OWASP Juice Shop*** is an open-source project hosted by the non-profit Open Web Application Security Project (OWASP) and is developed and maintained by volunteers. Check out the link below for more information and documentation on the project.

https://owasp-juice.shop

Help getting started | Dismiss

All Products



Apple Juice (1000ml)

1.99¤

Banana Juice (1000ml)

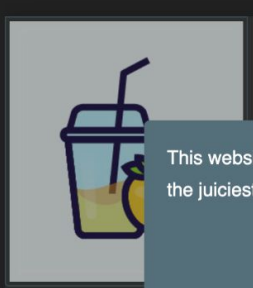
1.99¤

Best Juice Shop Salesman Artwork

5000¤

Carrot Juice (1000ml)

2.99¤



This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!

Me want it!

AppSec’s domain.

Secure the application code … SAST, DAST and secure coding practices.

Thank you.

OWASP Ottawa organizers and volunteers.

University of Ottawa

All my great colleagues at Rewind.