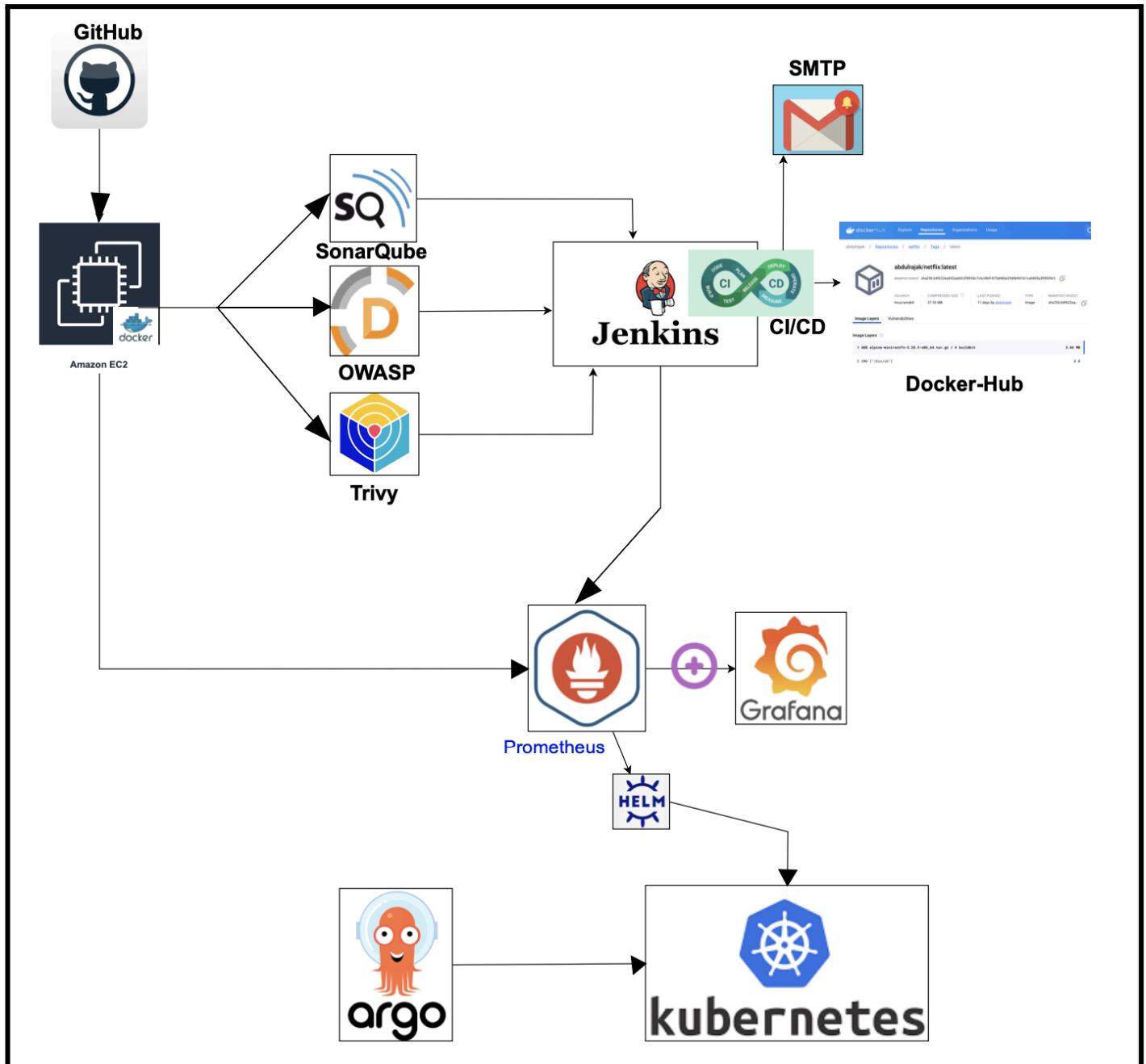


Deploying Netflix Clone on Cloud: A Complete DevSecOps Pipeline with Jenkins, GitHub, Docker, Amazon EC2, SonarQube, OWASP Dependency-Check, Trivy, ArgoCD, Helm, Kubernetes, Prometheus, Grafana, and Email Notifications!



Steps which I have followed for doing this task.

- **Initial Setup and Deployment**

Created the t2.large instance to handle all the workload of the project and dependencies, and cloned the Git repository to EC2.

Learn more about enabling ESM Apps service at <https://ubuntu.com/esm>

```
Last login: Mon Feb 24 18:16:05 2025 from 18.206.107.28
ubuntu@ip-172-31-32-200:~$ sudo su
root@ip-172-31-32-200:/home/ubuntu# cd DevSecOps-Project/
root@ip-172-31-32-200:/home/ubuntu/DevSecOps-Project# ls
Dockerfile Kubernetes README.md index.html package.json pipeline.txt public src tsconfig.json tsconfig.node.json vercel.json vite.config.ts yarn.lock
root@ip-172-31-32-200:/home/ubuntu/DevSecOps-Project#
```

Create the API from **TMDb**.

~ TMDb (The Movie Database) is a popular online database for movies, TV shows, and celebrities, providing detailed information and metadata.

Data from **TMDb** is used to generate the API.

- Create a Dockerfile, build the image using **docker build**, and test it locally using **docker run**.

Phase CI/CD Setup

```
root@ip-172-31-32-200:/home/ubuntu/DevSecOps-Project# docker images
REPOSITORY          TAG      IMAGE ID      CREATED     SIZE
<none>              <none>    daa383d400ca  10 days ago  858MB
<none>              <none>    22bca05c40de  10 days ago  858MB
<none>              <none>    7f7bc33e038f  10 days ago  858MB
<none>              <none>    127d0261867b  10 days ago  858MB
<none>              <none>    e0f28b4958f9  11 days ago  858MB
abdulrajak/netflix  latest   12edfadcb7f   11 days ago  56.5MB
netflix             latest   d9dd166a5970  13 days ago  56.5MB
<none>              <none>    a18b8b53fe50  13 days ago  844MB
nginx               stable-alpine  bb941add9a4c  2 weeks ago  47.2MB
sonarqube           lts-community 522e1399903e  5 weeks ago  604MB
node                16.17.0-alpine  5dcdf6157bd   2 years ago  115MB
root@ip-172-31-32-200:/home/ubuntu/DevSecOps-Project#
```

Install Jenkins for Automation:

Installing Jenkins and configuring SonarQube, Trivy, and OWASP in Jenkins for CI/CD.

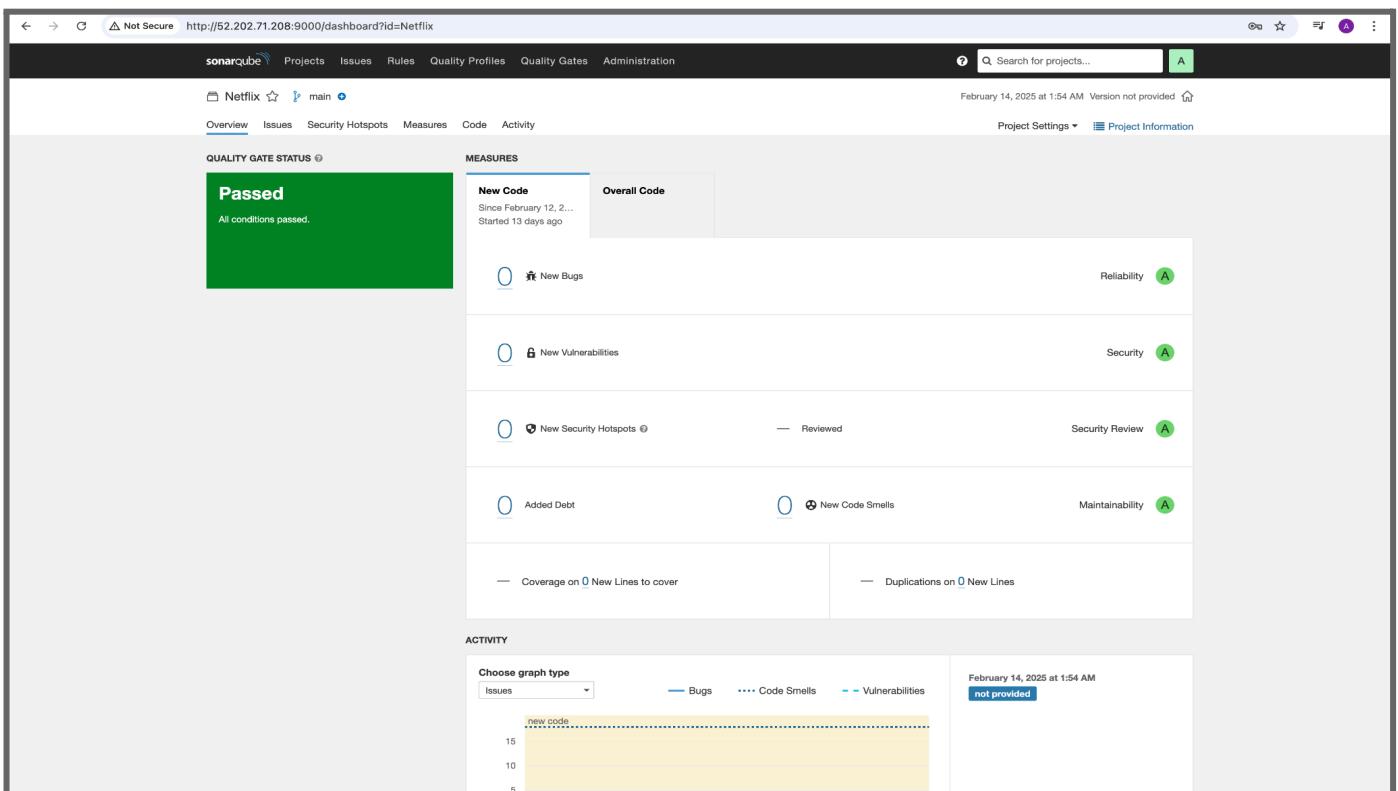
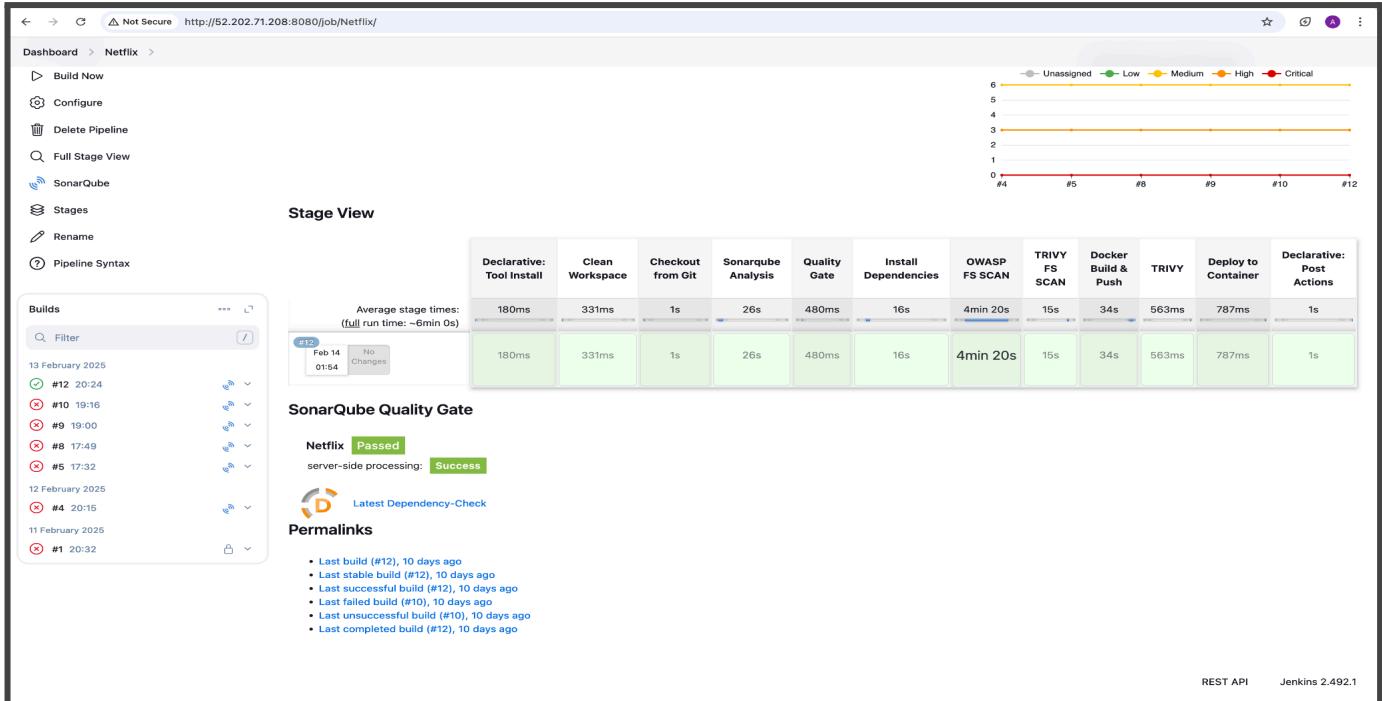
- Jenkins: An open-source automation server used for building, testing, and deploying applications in a CI/CD pipeline. It helps automate software development processes and integrates with various tools.
- SonarQube: A code quality and security analysis tool that scans code for vulnerabilities, bugs, and code smells. It ensures clean and maintainable code in the CI/CD pipeline.
- OWASP (Dependency-Check): A security tool that identifies known vulnerabilities in project dependencies. It helps mitigate security risks by ensuring third-party libraries are up to date and secure.

After successfully running the Jenkins pipeline, we can see the output like this:

Trivy is used in CI/CD for security and vulnerability scanning. Key reasons to use it:

- Container Security: Scans Docker images for vulnerabilities before deployment.
- Dependency Scanning: Detects security risks in open-source libraries and dependencies.
- Filesystem & Code Repository Scanning: Identifies misconfigurations and risks in infrastructure as code (IaC).

- Automation in CI/CD: Integrates with Jenkins, GitHub Actions, and other CI/CD tools for automated security checks.
- Compliance & Risk Management: Ensures applications meet security standards before production deployment.



SonarQube is used in CI/CD for code quality and security analysis. Key reasons to use it:

- Code Quality Analysis: Detects bugs, code smells, and maintainability issues in the codebase.
 - Security Vulnerability Detection: Identifies security flaws like SQL injection and XSS in the code.
 - Automated Code Review: Provides insights and recommendations to improve code quality.
 - Seamless CI/CD Integration: Works with Jenkins, GitLab, and other CI/CD tools for continuous scanning.
 - Compliance & Standards: Ensures adherence to coding standards and security best practices.

Not Secure http://52.202.71.208:9000/project/issues?id=Netflix&resolved=false

sonarqube Projects Issues Rules Quality Profiles Quality Gates Administration

Search for projects... A

Netflix main February 14, 2025 at 1:54 AM Version not provided

Overview Issues Security Hotspots Measures Code Activity Project Settings Project Information

My Issues All

Filters

Issues in new code

Type

- Bug 0
- Vulnerability 0
- Code Smell 18

Severity

- Blocker 0
- Critical 0
- Major 13
- Minor 5
- Info 0

Scope

Resolution

Status

Security Category

Creation Date

Language

Rule

Tag

Directory

File

Assignee

Author

Bulk Change

Dockerfile

Replace 'as' with upper case format 'AS'.

Code Smell Major Open Not assigned 5min effort Comment 2 years ago L1 % convention

src/components/GenreBreadcrumbs.tsx

Do not use Array index in keys

Code Smell Major Open Not assigned 5min effort Comment 2 years ago L28 % jsx, performance, react

src/components/GridWithInfiniteScroll.tsx

Do not use Array index in keys

Code Smell Major Open Not assigned 5min effort Comment 2 years ago L54 % jsx, performance, react

src/components/VideoItemWithHoverPure.tsx

Remove this commented out code. ☠

Code Smell Major Open Not assigned 5min effort Comment 1 year ago L33 % unused

Remove this commented out code. ☠

Code Smell Major Open Not assigned 5min effort Comment 1 year ago L37 % unused

src/components/VideoPortalContainer.tsx

'pageYOffset' is deprecated. This is a legacy alias of 'scrollY'.

Code Smell Minor Open Not assigned 15min effort Comment 2 years ago L58 % cwe, obsolete

src/components/slick-slider/SlickSlider.tsx

Do not use Array index in keys

Code Smell Major Open Not assigned 5min effort Comment 2 years ago L172 % jsx, performance, react

src/components/watch/VideoJSPlayer.tsx

Remove this commented out code. ☠

Code Smell Major Open Not assigned 5min effort Comment 1 year ago L23 % unused

Remove this commented out code. ☠

Code Smell Major Open Not assigned 5min effort Comment 1 year ago L47 % unused

Remove this commented out code. ☠

Code Smell Major Open Not assigned 5min effort Comment 1 year ago L61 % unused

Trivy scans the entire image, including OS packages and application dependencies, to detect vulnerabilities. It categorizes findings by severity (Critical, High, Medium, Low) and provides a detailed report for security risk mitigation.

```
59.41 MiB / 59.41 MiB [-----] 100.00% 25.80 MiB p/s 2.5s
2025-02-25T05:09:39Z INFO [vulndb] Artifact successfully downloaded      repo="mirror.gcr.io/aquasec/trivy-db:2"
2025-02-25T05:09:39Z INFO [vuln] Vulnerability scanning is enabled
2025-02-25T05:09:39Z INFO [secret] Secret scanning is enabled
2025-02-25T05:09:39Z INFO [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-02-25T05:09:39Z INFO [secret] Please see also https://aquasecurity.github.io/trivy/v0.59/docs/scanner/secret#recommendation for faster secret detection
2025-02-25T05:09:41Z INFO Detected OS   family="alpine" version="3.20.5"
2025-02-25T05:09:41Z INFO [alpine] Detecting vulnerabilities... os_version="3.20" repository="3.20" pkg_num=66
2025-02-25T05:09:41Z INFO Number of language-specific files    num=0
2025-02-25T05:09:41Z WARN Using severities from other vendors for some vulnerabilities. Read https://aquasecurity.github.io/trivy/v0.59/docs/scanner/vulnerability#severity-selection for details.

12edfad6b7f (alpine 3.20.5)

Total: 12 (UNKNOWN: 4, LOW: 2, MEDIUM: 4, HIGH: 2, CRITICAL: 0)
```

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
curl	CVE-2025-0725	MEDIUM	fixed	8.11.1-r0	8.12.0-r0	libcurl: Buffer Overflow in libcurl via zlib Integer Overflow https://avd.aquasec.com/nvd/cve-2025-0725
	CVE-2025-0167	LOW				When asked to use a `.netrc` file for credentials **and** to follow... https://avd.aquasec.com/nvd/cve-2025-0167
	CVE-2025-0665	UNKNOWN				libcurl would wrongly close the same eventfd file descriptor twice whe https://avd.aquasec.com/nvd/cve-2025-0665
libcrypto3	CVE-2024-12797	HIGH	3.3.2-r1	3.3.3-r0	openssl: RFC7250 handshakes with unauthenticated servers don't abort as expected https://avd.aquasec.com/nvd/cve-2024-12797	
	CVE-2024-13176	MEDIUM			3.3.2-r2	openssl: Timing side-channel in ECDSA signature computation https://avd.aquasec.com/nvd/cve-2024-13176
libcurl	CVE-2025-0725		8.11.1-r0	8.12.0-r0	8.12.0-r0	libcurl: Buffer Overflow in libcurl via zlib Integer Overflow https://avd.aquasec.com/nvd/cve-2025-0725
	CVE-2025-0167	LOW				When asked to use a `.netrc` file for credentials **and** to follow... https://avd.aquasec.com/nvd/cve-2025-0167
	CVE-2025-0665	UNKNOWN				libcurl would wrongly close the same eventfd file descriptor twice whe https://avd.aquasec.com/nvd/cve-2025-0665
libssl3	CVE-2024-12797	HIGH	3.3.2-r1	3.3.3-r0	openssl: RFC7250 handshakes with unauthenticated servers don't abort as expected https://avd.aquasec.com/nvd/cve-2024-12797	
	CVE-2024-13176	MEDIUM			3.3.2-r2	openssl: Timing side-channel in ECDSA signature computation https://avd.aquasec.com/nvd/cve-2024-13176
musl	CVE-2025-26519	UNKNOWN	1.2.5-r0	1.2.5-r1	musl libc 0.9.13 through 1.2.5 before 1.2.6 has an out-of-bounds write	https://avd.aquasec.com/nvd/cve-2025-26519
musl-utils						

Dependency-Check Results

Not Secure http://52.202.71.208:8080/job/Netflix/4/dependency-check-findings/ Jenkins admin log out

Dashboard > Netflix > #4 > Dependency-Check

Dependency-Check Results

SEVERITY DISTRIBUTION

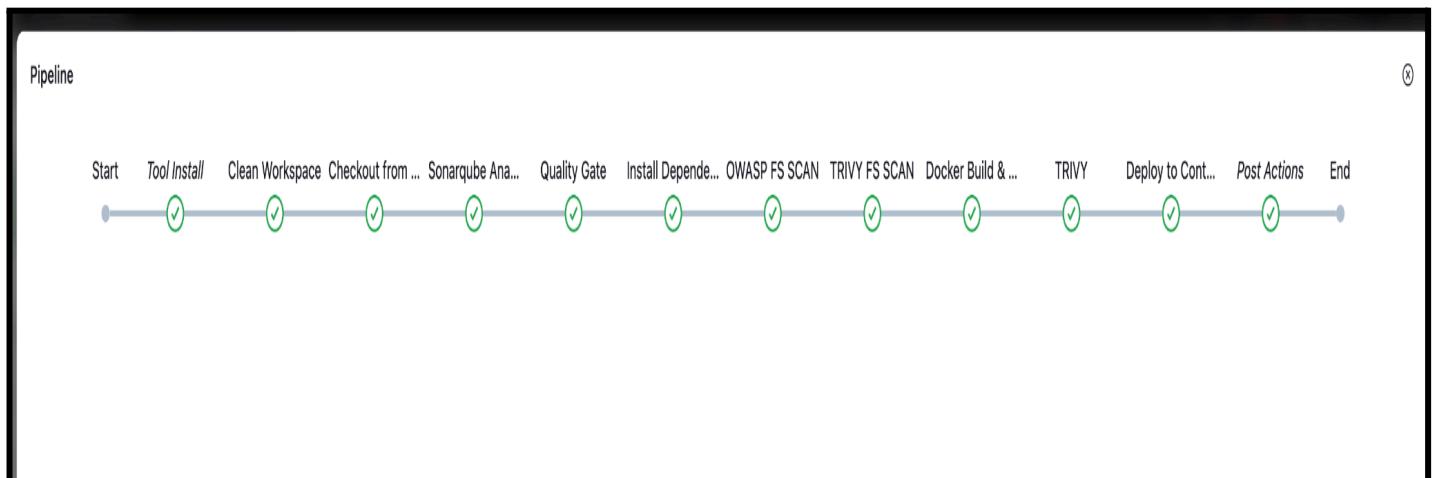
Severity	Count
Low	3
Medium	6
High	2

Search

File Name	Vulnerability	Severity	Weakness
nanoid:3.3.4	OSSINDEX CVE-2024-55565	Medium	CWE-835
postcss:8.4.18	NVD CVE-2023-44270	Medium	CWE-74
rollup:2.79.1	NVD CVE-2024-47068	Medium	CWE-79
vite:3.2.2	OSSINDEX CVE-2024-45811	High	CWE-200
vite:3.2.2	NVD CVE-2023-34092	High	CWE-50
vite:3.2.2	NVD CVE-2024-23331	High	CWE-284
vite:3.2.2	OSSINDEX CVE-2024-31207	Medium	CWE-200
vite:3.2.2	OSSINDEX CVE-2025-24010	Medium	CWE-1385
vite:3.2.2	OSSINDEX CVE-2024-45812	Medium	CWE-79

Status Changes Console Output Edit Build Information Delete build '#4' Timings Git Build Data Dependency-Check Pipeline Overview Pipeline Console Restart from Stage Replay Pipeline Steps Workspaces Previous Build Next Build Jenkins 2.492.1

Pipeline overview



Docker images are pushed to Docker Hub in the specified repository using the `docker push` command after proper tagging. This ensures the image is stored remotely and can be pulled for deployment across different environments.

The screenshot shows the Docker Hub interface for the repository `abdulrajak/netflix`. The page displays the `latest` tag of the image. Key details shown include:

- Image Details:** `abdulrajak/netflix:latest`
- Manifest Digest:** `sha256:b4f622ea692ae0c2f893dc7c6c4841875d480e29d0b941b1ca08d5a39900fe5`
- OS/ARCH:** `linux/amd64`
- Compressed Size:** `27.55 MB`
- Last Pushed:** `11 days by abdulrajak`
- Type:** `Image`
- Manifest Digest:** `sha256:b4f622ea692ae0c2f893dc7c6c4841875d480e29d0b941b1ca08d5a39900fe5`

Image Layers: The image consists of 12 layers, each with its corresponding command and size. The commands are:

- `ADD alpine-minirootfs-3.20.5-x86_64.tar.gz / # buildkit` (3.46 MB)
- `CMD ["bin/sh"]` (0 B)
- `LABEL maintainer=NGINX Docker Maintainers <docker-maint@nginx.com>` (0 B)
- `ENV NGINX_VERSION=1.26.3` (0 B)
- `ENV PKG_RELEASE=1` (0 B)
- `ENV DYNPKG_RELEASE=2` (0 B)
- `RUN /bin/sh -c set -x` (1.67 MB)
- `COPY docker-entrypoint.sh / # buildkit` (627 B)
- `COPY 10-listen-on-ipv6-by-default.sh /docker-entrypoint.d # buildkit` (955 B)
- `COPY 15-local-resolvers.envsh /docker-entrypoint.d # buildkit` (404 B)
- `COPY 20-envsubst-on-templates.sh /docker-entrypoint.d # buildkit` (1.18 KB)
- `COPY 30-tune-worker-processes.sh /docker-entrypoint.d # buildkit` (1.36 KB)

Command: A text input field containing the command `ADD alpine-minirootfs-3.20.5-x86_64.tar.gz / # buildkit`.

Phase Monitoring:

Node Exporter: Collects and exposes system-level metrics like CPU, memory, and disk usage. It runs as an agent on the server and depends on Prometheus to scrape and store these metrics. Without Node Exporter, Prometheus cannot collect server-level data.

Metric Collection: Node Exporter gathers system-level metrics such as CPU, memory, disk, and network usage from the host machine.

Data Exposure: It makes these metrics available at <http://<server-ip>:9100/metrics> in a Prometheus-compatible format.

Integration with Prometheus: Prometheus scrapes these exposed metrics at regular intervals for monitoring and alerting.

```

# HELP go_gc_duration_seconds A summary of the wall-time pause (stop-the-world) duration in garbage collection cycles.
# TYPE go_gc_duration_seconds summary
go_gc_duration_seconds{quantile="0"} 1.5986e-05
go_gc_duration_seconds{quantile="0.25"} 2.3791e-05
go_gc_duration_seconds{quantile="0.5"} 2.5645e-05
go_gc_duration_seconds{quantile="0.75"} 2.9211e-05
go_gc_duration_seconds{quantile="1"} 0.000127933
go_gc_duration_seconds_sum 0.00019431
go_gc_duration_seconds_count 68
# HELP go_gc_golang_percent Heap size target percentage configured by the user, otherwise 100. This value is set by the GOGC environment variable, and the runtime/debug.SetGCPercent function. Sourced from /gc/golang:percent
# TYPE go_gc_golang_percent gauge
go_gc_golang_percent 100
# HELP go_gc_gomemlimit_bytes Go runtime memory limit configured by the user, otherwise math.MaxInt64. This value is set by the GOMEMLIMIT environment variable, and the runtime/debug.SetMemoryLimit function. Sourced from /gc/gomemlimit:bytes
# TYPE go_gc_gomemlimit_bytes gauge
go_gc_gomemlimit_bytes 9.223372036854776e+18
# HELP go_goroutines Number of goroutines that currently exist.
# TYPE go_goroutines gauge
go_goroutines 7
# HELP go_info Information about the Go environment.
# TYPE go_info gauge
go_info{version="go1.23.6"} 1
# HELP go_memstats_alloc_bytes Number of bytes allocated in heap and currently in use. Equals to /memory/classes/heap/objects:bytes.
# TYPE go_memstats_alloc_bytes gauge
go_memstats_alloc_bytes 697776
# HELP go_memstats_alloc_bytes_total Total number of bytes allocated in heap until now, even if released already. Equals to /gc/heap/allocs:bytes.
# TYPE go_memstats_alloc_bytes_total counter
go_memstats_alloc_bytes_total 1.5369032e+07
# HELP go_memstats_buck_hash_sys_bytes Number of bytes used by the profiling bucket hash table. Equals to /memory/classes/profiling/buckets:bytes.
# TYPE go_memstats_buck_hash_sys_bytes gauge
go_memstats_buck_hash_sys_bytes 1.449567e+06
# HELP go_memstats_frees_total Total number of heap objects frees. Equals to /gc/heap/frees:objects + /gc/heap/tiny/allocs:objects.
# TYPE go_memstats_frees_total counter
go_memstats_frees_total 172085
# HELP go_memstats_gc_sys_bytes Number of bytes used for garbage collection system metadata. Equals to /memory/classes/metadata/other:bytes.
# TYPE go_memstats_gc_sys_bytes gauge
go_memstats_gc_sys_bytes 2.986568e+06
# HELP go_memstats_heap_alloc_bytes Number of heap bytes allocated and currently in use, same as go_memstats_alloc_bytes. Equals to /memory/classes/heap/objects:bytes.
# TYPE go_memstats_heap_alloc_bytes gauge
go_memstats_heap_alloc_bytes 697776
# HELP go_memstats_heap_idle_bytes Number of heap bytes waiting to be used. Equals to /memory/classes/heap/released:bytes + /memory/classes/heap/free:bytes.
# TYPE go_memstats_heap_idle_bytes gauge
go_memstats_heap_idle_bytes 5.840896e+06
# HELP go_memstats_heap_inuse_bytes Number of heap bytes that are in use. Equals to /memory/classes/heap/objects:bytes + /memory/classes/heap/unused:bytes
# TYPE go_memstats_heap_inuse_bytes gauge
go_memstats_heap_inuse_bytes 1.990656e+06
# HELP go_memstats_heap_objects Number of currently allocated objects. Equals to /gc/heap/objects:objects.
# TYPE go_memstats_heap_objects gauge
go_memstats_heap_objects 4466
# HELP go_memstats_heap_released_bytes Number of heap bytes released to OS. Equals to /memory/classes/heap/released:bytes.
# TYPE go_memstats_heap_released_bytes gauge
go_memstats_heap_released_bytes 5.169152e+06
# HELP go_memstats_heap_sys_bytes Number of heap bytes obtained from system. Equals to /memory/classes/heap/objects:bytes + /memory/classes/heap/unused:bytes + /memory/classes/heap/released:bytes + /memory/classes/heap/free:bytes.
# TYPE go_memstats_heap_sys_bytes gauge
go_memstats_heap_sys_bytes 7.831552e+06
# HELP go_memstats_last_gc_time_seconds Number of seconds since 1970 of last garbage collection.
# TYPE go_memstats_last_gc_time_seconds gauge
go_memstats_last_gc_time_seconds 1.740307196418118e+09
# HELP go_memstats_mallocs_total Total number of heap objects allocated, both live and gc-ed. Semantically a counter version for go_memstats_heap_objects gauge. Equals to /gc/heap/allocs:objects + /gc/heap/tiny/allocs:objects.
# TYPE go_memstats_mallocs_total counter
go_memstats_mallocs_total 176551
# HELP go_memstats_mcache_inuse_bytes Number of bytes in use by mcache structures. Equals to /memory/classes/metadata/mcache/inuse:bytes.
# TYPE go_memstats_mcache_inuse_bytes gauge
go_memstats_mcache_inuse_bytes 1200
# HELP go_memstats_mcache_sys_bytes Number of bytes used for mcache structures obtained from system. Equals to /memory/classes/metadata/mcache/inuse:bytes + /memory/classes/metadata/mcache/free:bytes.
# TYPE go_memstats_mcache_sys_bytes gauge
go_memstats_mcache_sys_bytes 15600

```

Prometheus: A monitoring system that scrapes metrics from Node Exporter and other sources, storing them as time-series data. It relies on exporters to gather data and depends on Grafana for visualization. Prometheus also provides querying and alerting capabilities.

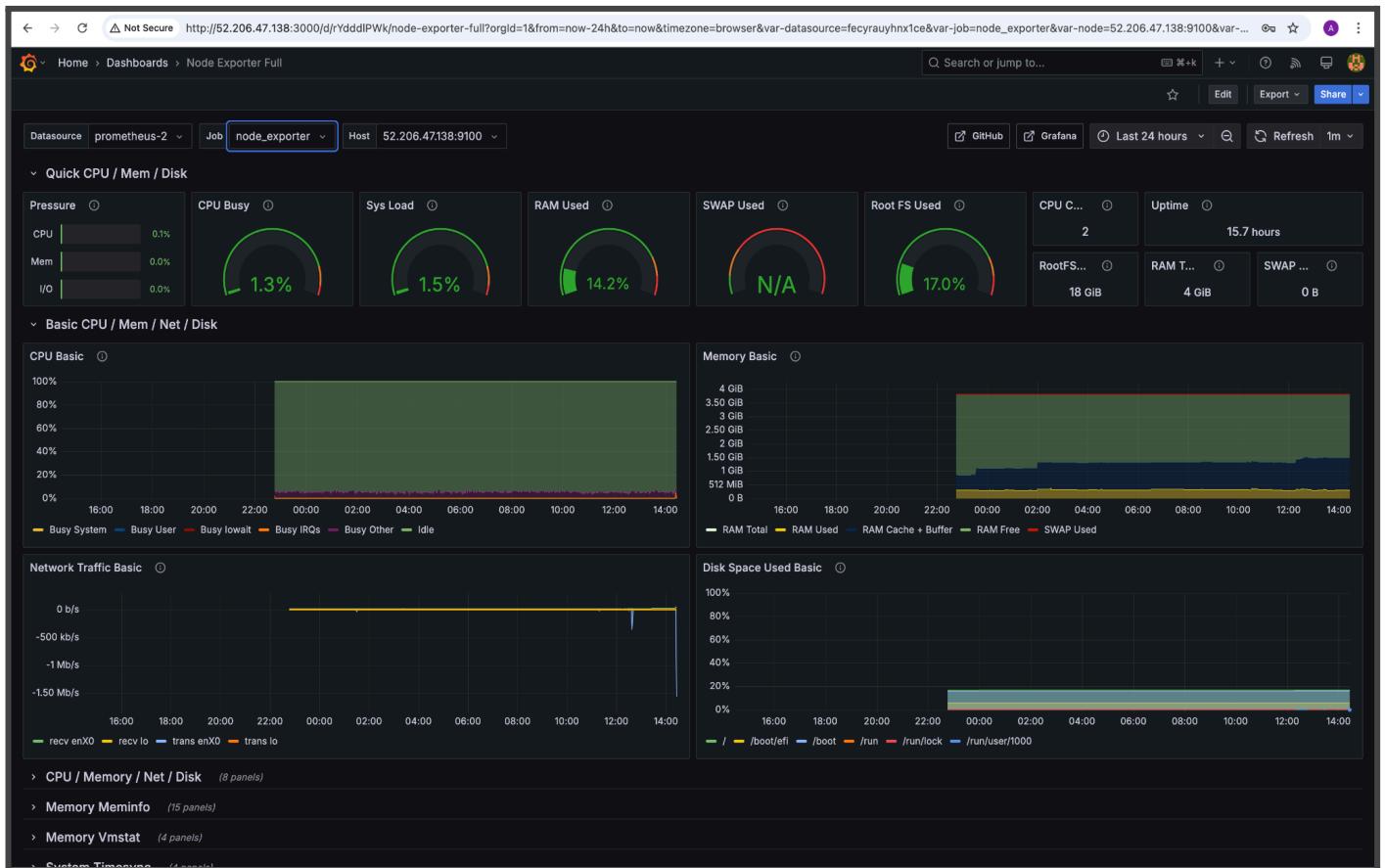
The screenshot shows the Prometheus Targets page with the URL <http://52.206.47.138:9090/targets?search=>. The page has a dark header with the Prometheus logo and navigation links for Alerts, Graph, Status, and Help. Below the header is a search bar and a filter section with buttons for All, Unhealthy, Collapse All, Unknown, Unhealthy, and Healthy. The main content area is titled "Targets" and lists four service entries:

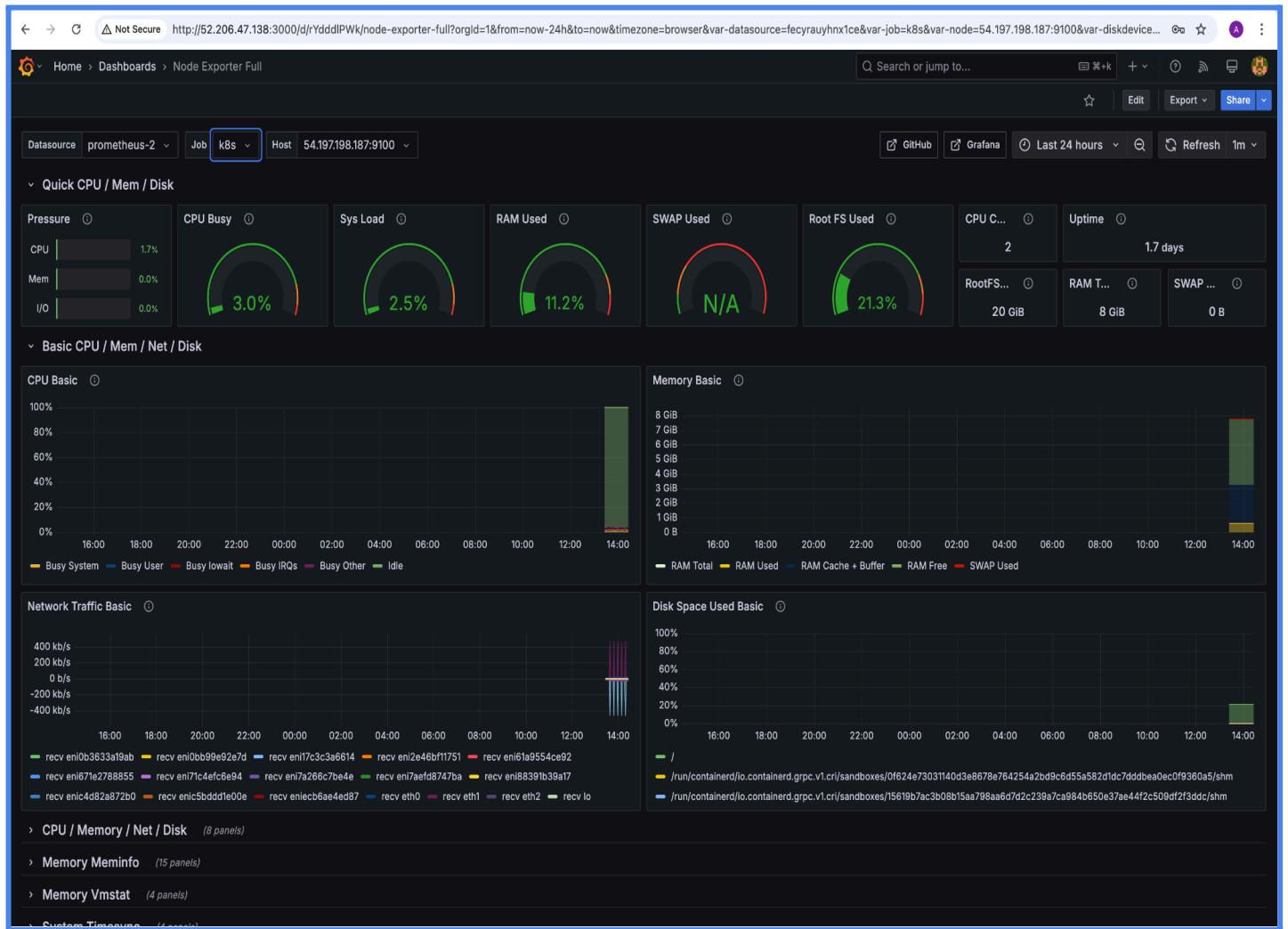
- jenkins (1/1 up)**: Shows one endpoint at <http://52.202.71.208:8080/prometheus> in UP state, last scraped 12.201s ago, with a scrape duration of 12.432ms. Labels: instance="52.202.71.208:8080", job="jenkins".
- k8s (1/1 up)**: Shows one endpoint at <http://54.197.198.187:9100/metrics> in UP state, last scraped 8.563s ago, with a scrape duration of 26.262ms. Labels: instance="54.197.198.187:9100", job="k8s".
- node_exporter (1/1 up)**: Shows one endpoint at <http://52.206.47.138:9100/metrics> in UP state, last scraped 14.315s ago, with a scrape duration of 13.526ms. Labels: instance="52.206.47.138:9100", job="node_exporter".
- prometheus (1/1 up)**: Shows one endpoint at <http://localhost:9090/metrics> in UP state, last scraped 3.940s ago, with a scrape duration of 4.776ms. Labels: instance="localhost:9090", job="prometheus".

Extracted node metrics, including CPU, memory, and other system resources, using Node Exporter. The Prometheus container is running and scraping these metrics for monitoring. Additionally, services like Jenkins, Kubernetes, and other installed applications are also monitored through Prometheus.

Grafana is a visualization tool that provides interactive dashboards for monitoring metrics collected by Prometheus.

- It connects to Prometheus as a data source and queries stored metrics to generate real-time graphs and alerts.
- Grafana allows users to create custom dashboards with various panels, thresholds, and alerting rules.
- It supports multiple data sources, including Prometheus, Loki, Elasticsearch, and more.
- With role-based access control, teams can collaborate on monitoring and troubleshooting efficiently





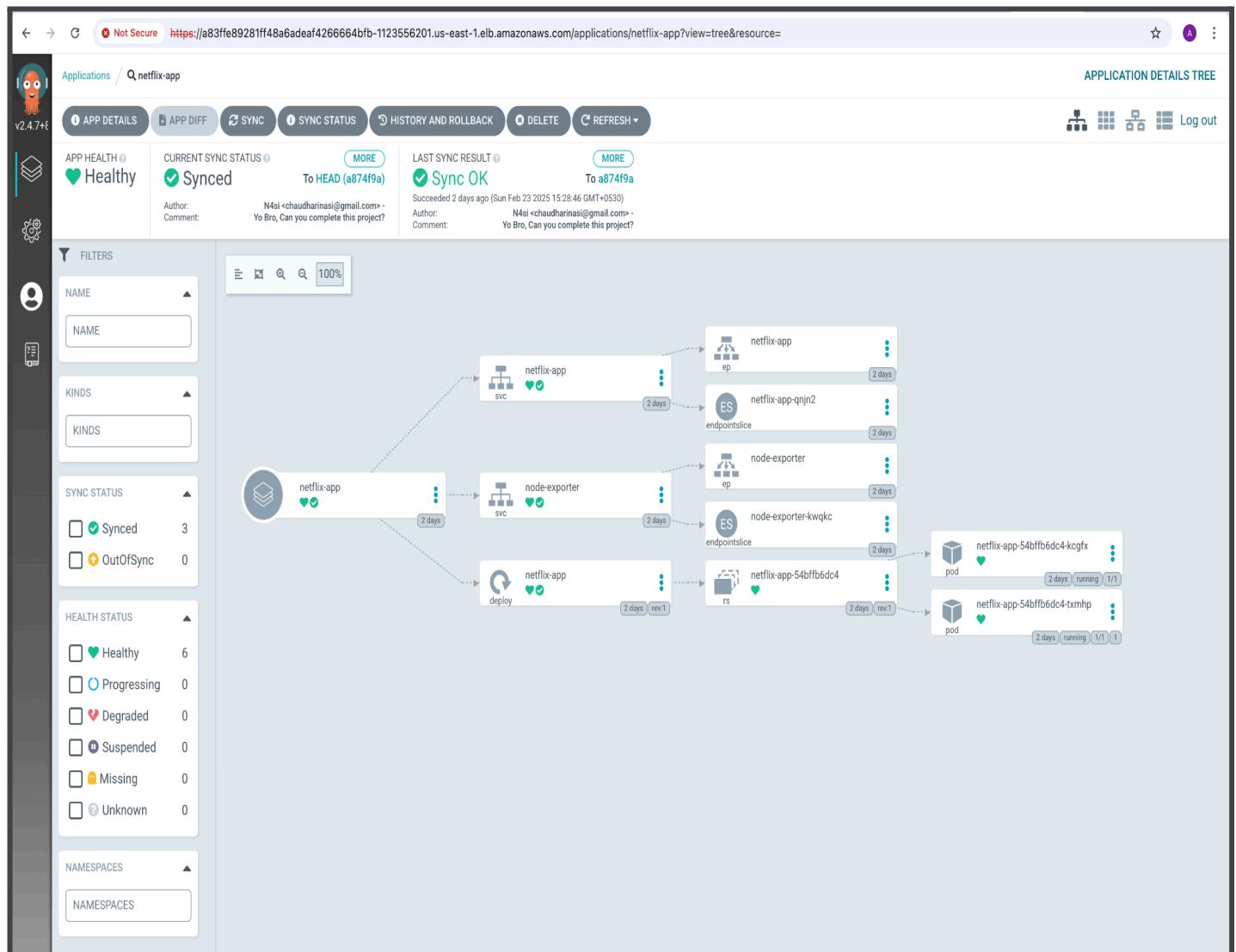
Docker hub :

abdulrajak/netflix:latest > Public Image

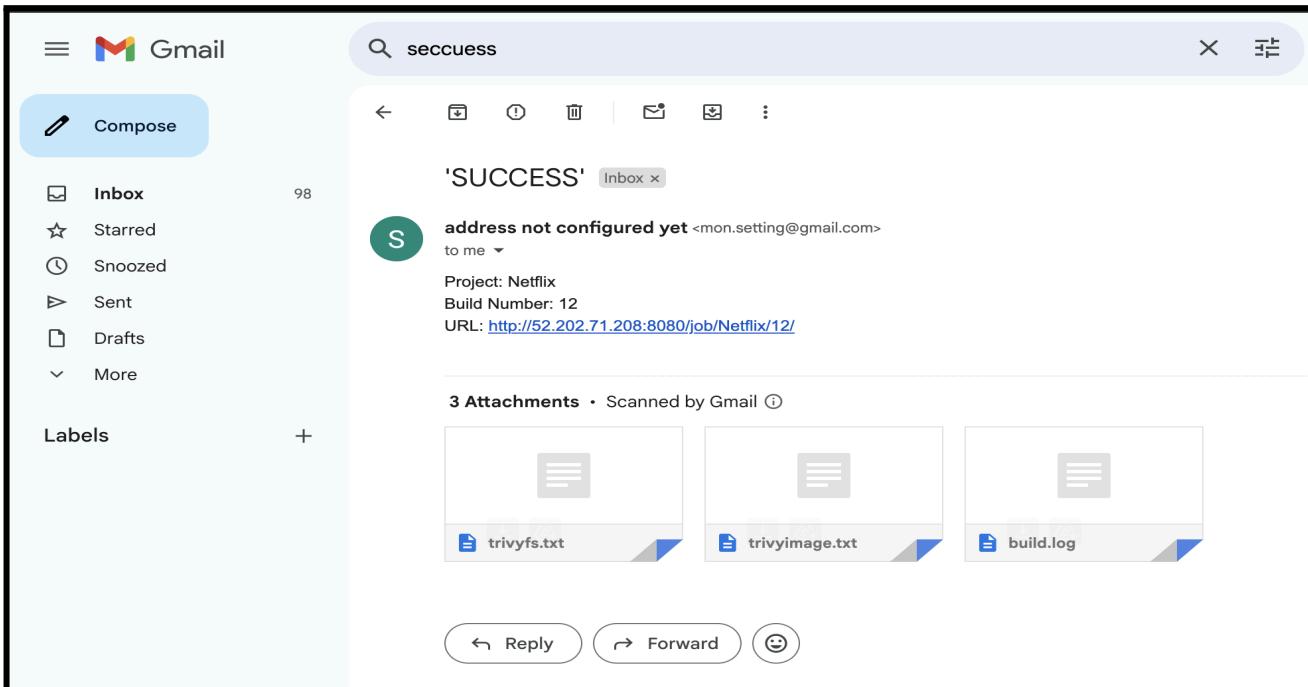
Argo CD is a declarative, GitOps-based continuous delivery tool for Kubernetes that automates application deployment and management. It ensures the cluster state remains in sync with the desired state defined in a Git repository.

Key Features:

- Automated Sync – Continuously syncs Kubernetes manifests from Git to maintain the desired state.
- Rollback & History – Supports rollbacks and maintains deployment history for quick recovery.
- Application Health Monitoring – Provides real-time visibility into application status and health.



After successfully completing the CI/CD pipeline at every stage, I integrated **SMTP** for email notifications. This setup ensures that Trivy scans images or containers and sends reports via email.



For OSS Maintainers: VEX Notice						

If you're an OSS maintainer and Trivy has detected vulnerabilities in your project that you believe are not actually exploitable, consider issuing a VEX (Vulnerability Exploitability eXchange) statement.						
VEX allows you to communicate the actual status of vulnerabilities in your project, improving security transparency and reducing false positives for your users.						
Learn more and start using VEX: https://aquasecurity.github.io/trivy/v0.59/docs/supply-chain/vex/repo#publishing-vex-documents						
To disable this notice, set the TRIVY_DISABLE_VEX_NOTICE environment variable.						
package-lock.json (npm)						
=====						
Total: 10 (UNKNOWN: 0, LOW: 0, MEDIUM: 7, HIGH: 3, CRITICAL: 0)						
Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
esbuild	GHSA-67mh-4wv8-2f99	MEDIUM	fixed	0.15.12	0.25.0	esbuild enables any website to send any requests to the development server...
GHSA-67mh-4wv8-2f99						https://github.com/advisories/
nanoid	CVE-2024-55565			3.3.4	5.0.9, 3.3.8	nanoid: nanoid mishandles non-integer values https://avd.aquasec.com/nvd/cve-2024-55565
postcss	CVE-2023-44270			8.4.18	8.4.31	PostCSS: Improper input validation in PostCSS https://avd.aquasec.com/nvd/cve-2023-44270
rollup	CVE-2024-47068	HIGH		2.79.1	3.29.5, 4.22.4, 2.79.2	rollup: DOM Clobbering Gadget found in rollup bundled scripts that leads to... https://avd.aquasec.com/nvd/cve-2024-47068
vite	CVE-2023-34092			3.2.2	2.9.16, 3.2.7, 4.0.5, 4.1.5, 4.2.3, 4.3.9	Vite Server Options (server.fs.deny) can be bypassed using double forward-slash (//) https://avd.aquasec.com/nvd/cve-2023-34092

Finally, we can see the Netflix homepage deployed on Kubernetes (K8s) clusters.

Key Points:

- The deployment is managed via Argo CD for GitOps-based continuous delivery.
- Services are exposed using Kubernetes networking, ensuring accessibility.

