DevOps, Software Evolution & Software Maintenance

The Eagles (Group H)

Trond Pingel Anchær Rossing (trro@itu.dk)
Roman Zvoda (rozv@itu.dk)
Rasmus Balder Nordbjærg (rano@itu.dk)
Daniel Spandet Grønbjerg (dangr@itu.dk)
Jan Lishak (jlis@itu.dk)

May 21, 2024

Contents

1. Introduction

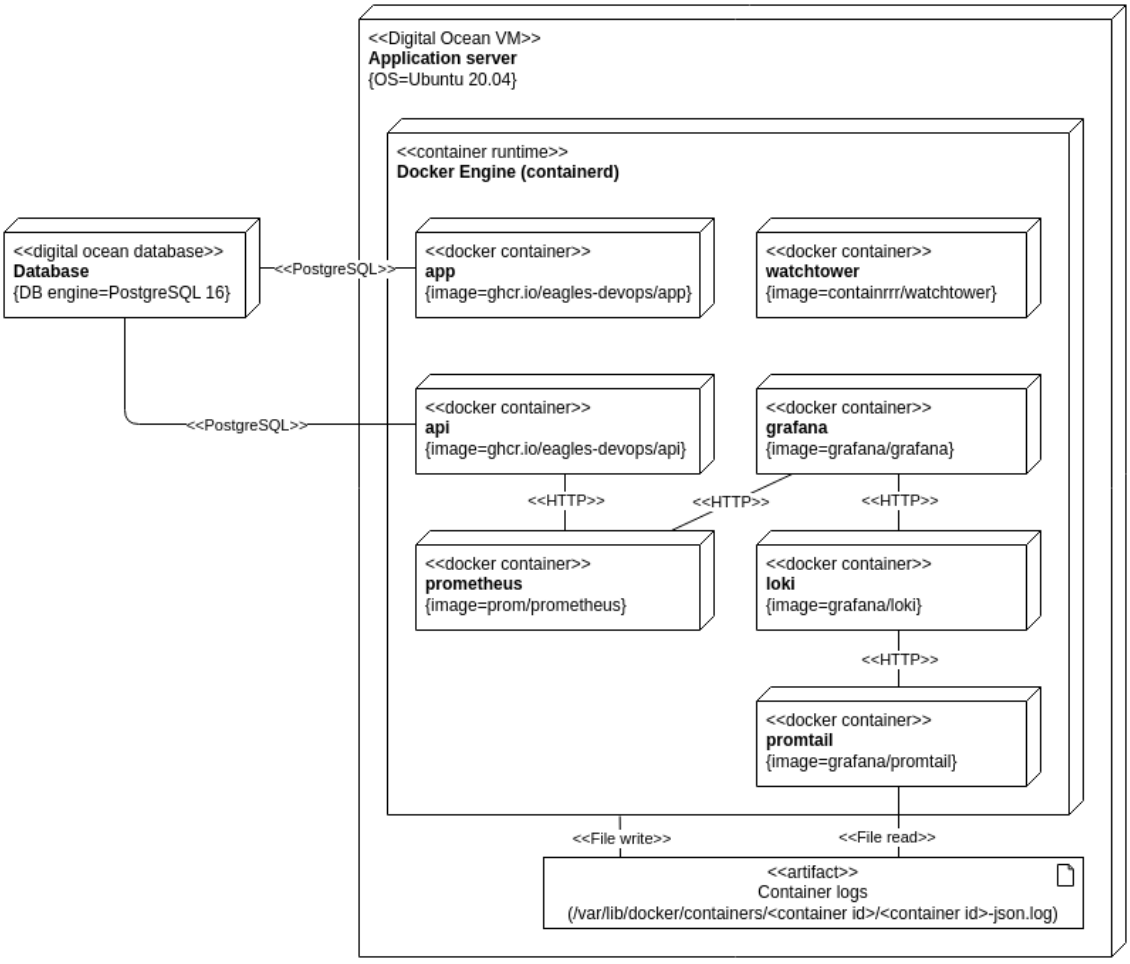
The project focuses on building and maintaining a mock version of Twitter called **MiniTwit** by applying various DevOps techniques such as automation, cloud deployment, scaling, maintainability, monitoring, testing, and others. The initial web application, which was outdated with the latest technologies and was not following any standard practices, was rewritten from the ground up and gradually equipped with automations and improvements so that it became able to process a high load of incoming requests to the app.

2. System's Perspective

The documentation of the architecture differentiates between the old and the new architecture. The old architecture was reliable, however there were single points of faulre. The upgraded architecture resolves some of those issues by introducing load-balancing.

Old architecture

The below diagram shows the deployment diagram for the different components of an earlier design of the system. At the end of the project this setup was still in use however the system was in process of being migrated to the new architecture explained later in the report.



The 2 main parts of the system are the the database and the server. The database is a managed PostgreSQL database from digital ocean. The components shown in the digram were all defined in a docker-compose file.

New architecture

Below diagram shows the new architecture

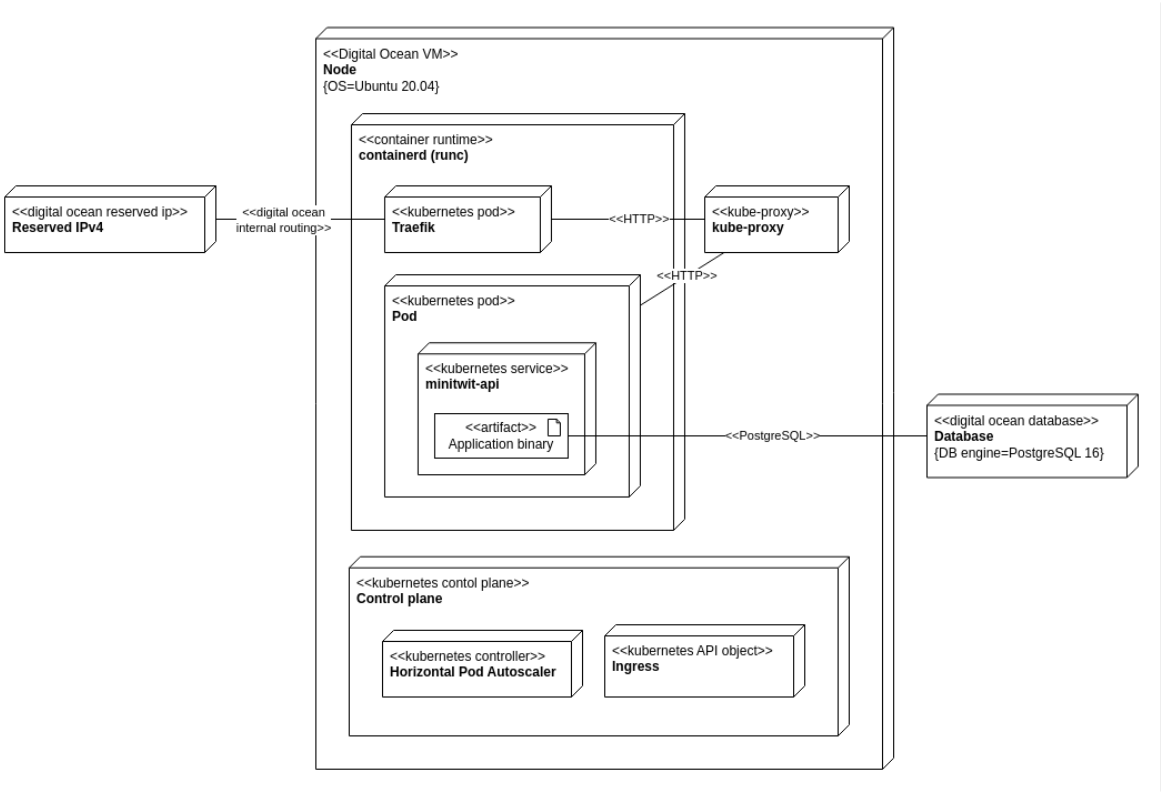


Figure 1: Deployment View: New architecture

Old Setup

Before we introducted Kubernetes

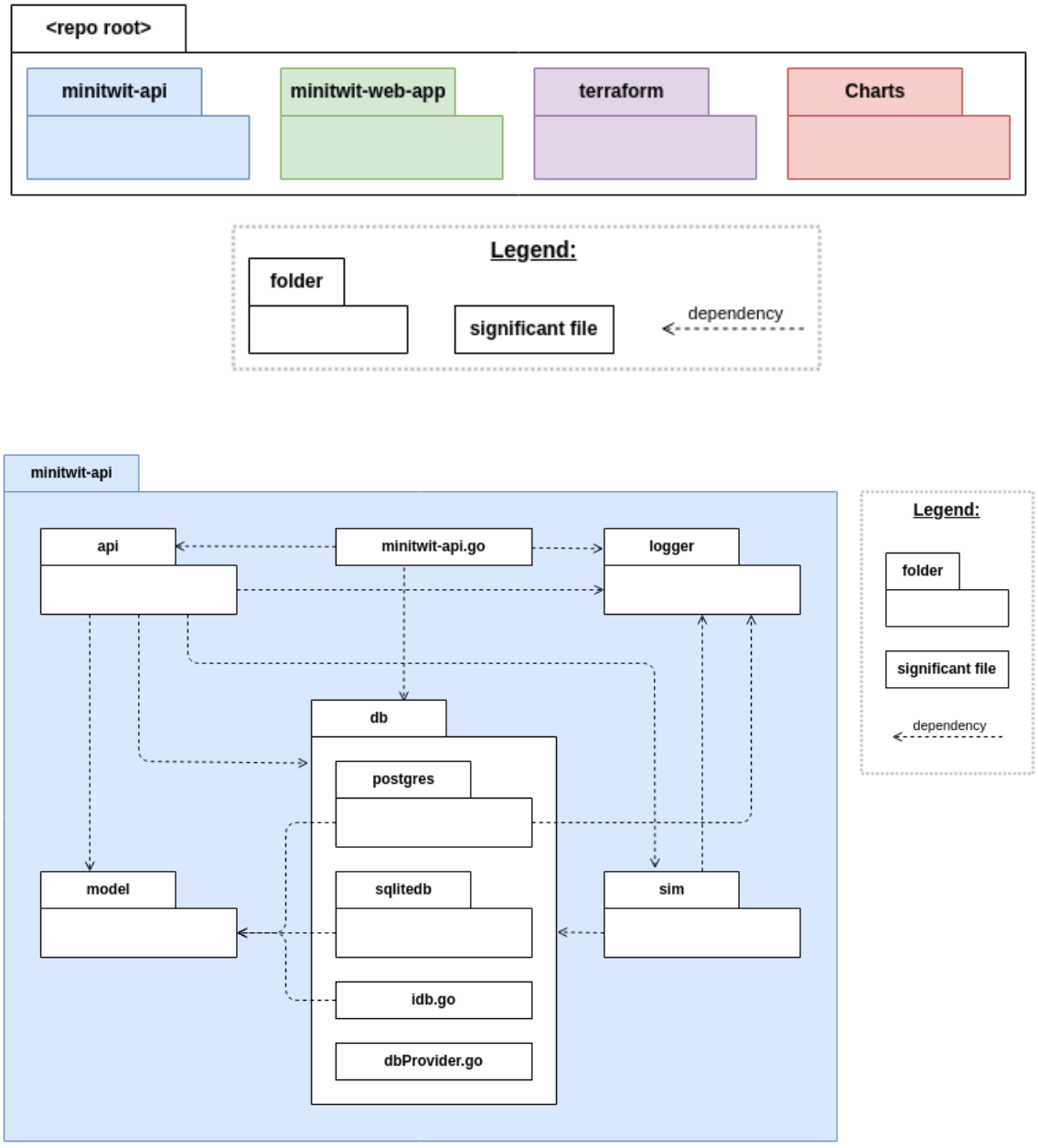


Figure 2: Module View: API

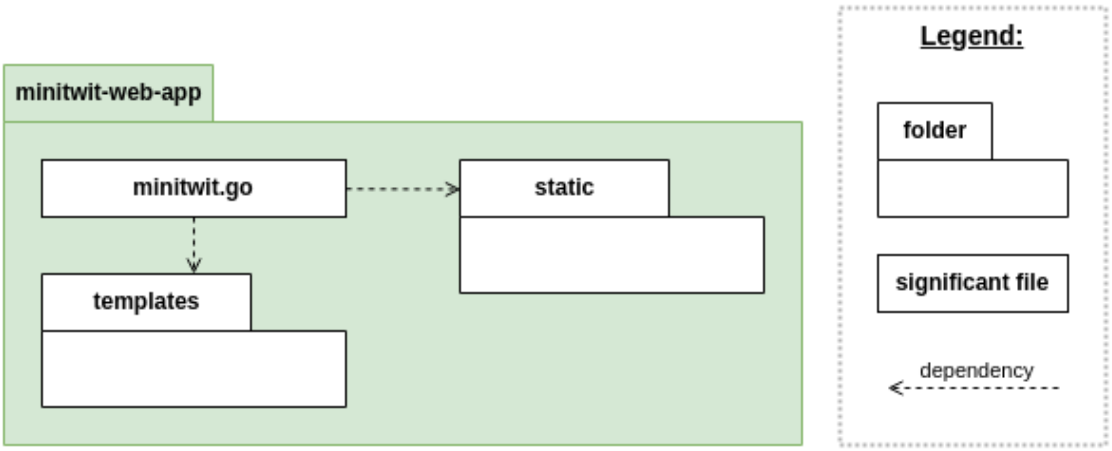


Figure 3: Module View: Web App

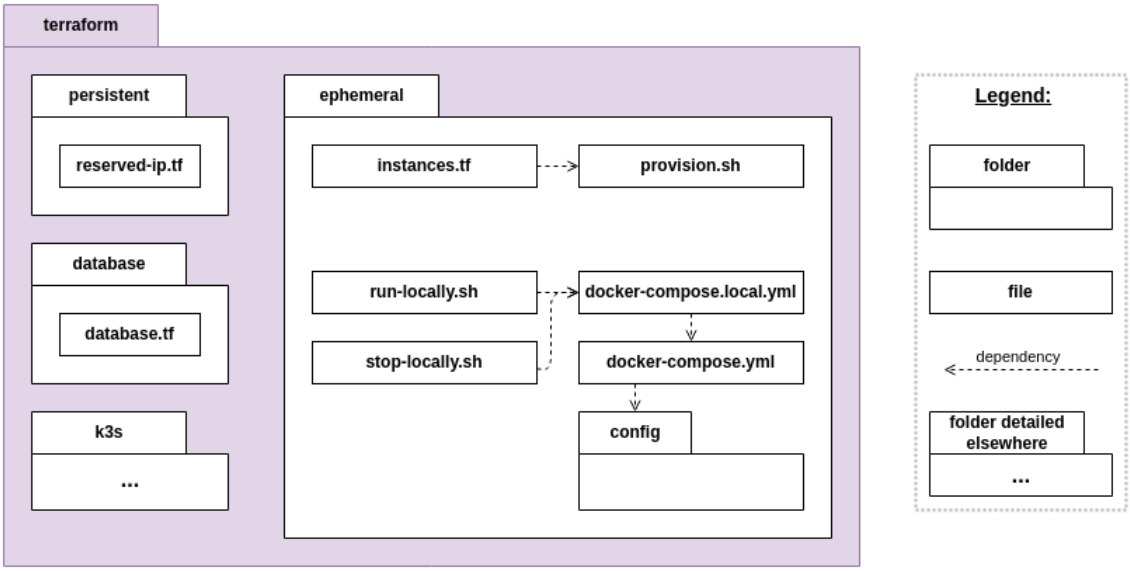
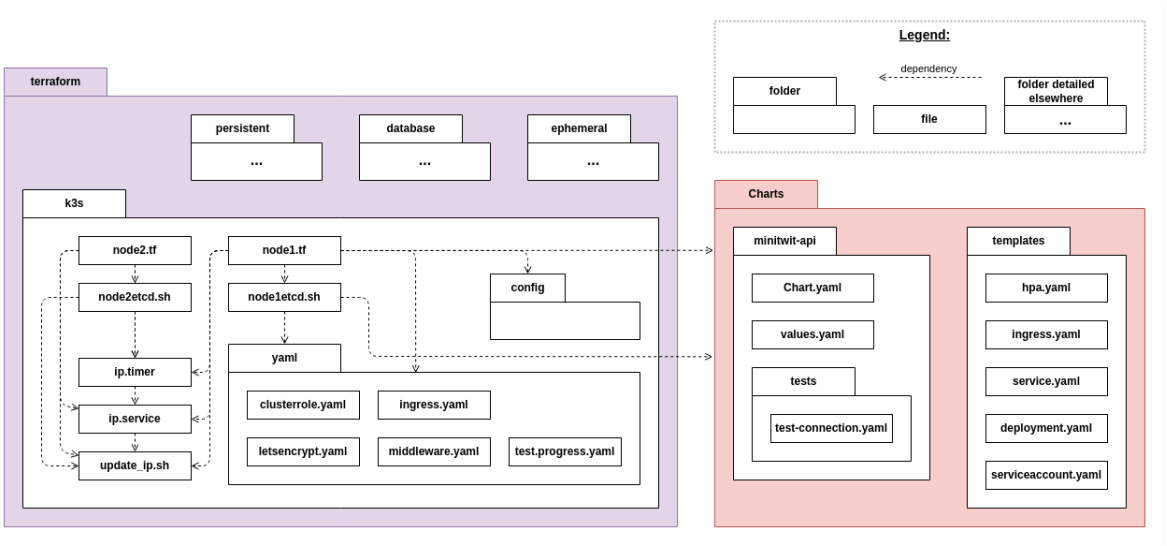


Figure 4: Module View: Terraform old

New setup

After we introducted Kubernetes



K3S

The API is now running on a leightweight Kubernetes cluster - k3s. This cluster spans two Server nodes. The cluster is spun up from scratch using terraform, and the infrastructure takes about an hour to spin up, as it needs to wait for dns propagation to be able to confirm domain ownership for the SSL certificate. Configuration and secrets are deployed in the cluster as part of the setup process.

When Kubernetes was chosen rather than an arguably easier option like docker swarm, it stems from Kubernetes being the industry standard. Docker swarm is nice for showing simple scaling of containers, but Kubernetes seemed like an interesting challenge. The complexity of Kubernetes has proven quite time consuming, and we didn't manage to move as many things as we would have liked to the cluster.

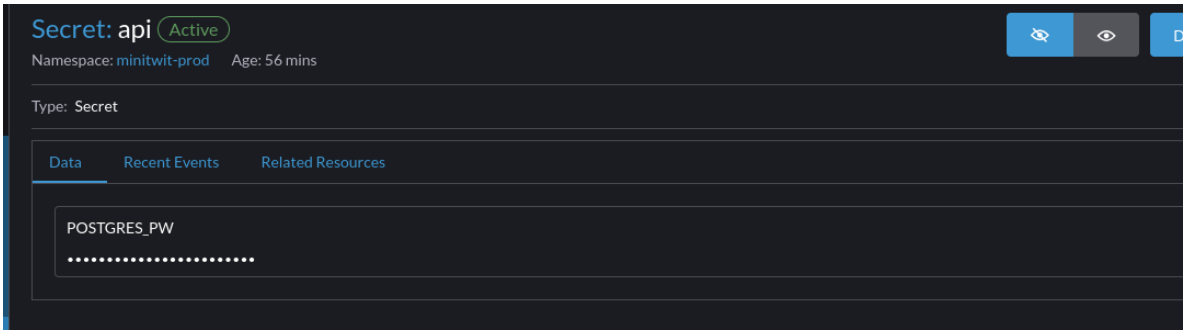


Figure 5: secret

Rancher is running on top to provide a nice UI for management.

Letsencrypt is used for SSL certificates and is automatically created/renewed for deployments.

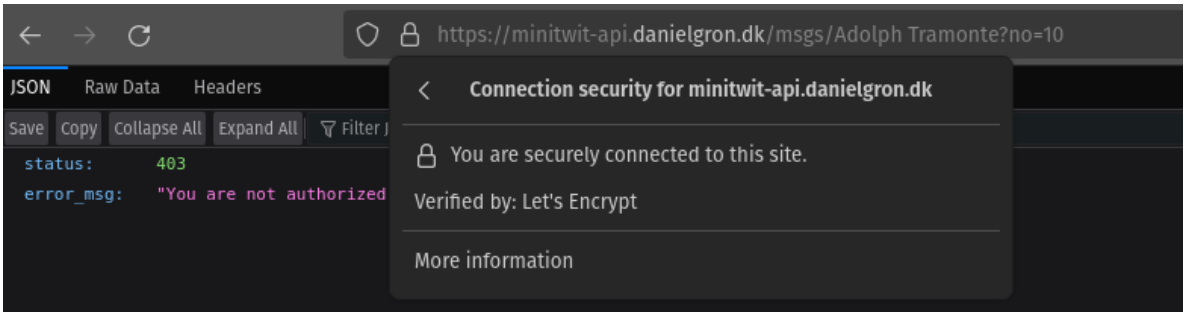


Figure 6: ssl

Scaling and upgrades

When deployed on the Kubernetes cluster, the api will be deployed with 2 instances using blue/green deployment, which ensures no downtime when deploying. It uses a very basic health check that requires the database connection to be established. The ingress will not point to the new instance until this check passes.

Once a container with the new image is up and running a coresponding pod based on the old image is terminated.

Autoscaling is enabled for the deployment, meaning that if load for a pod exceeds the treshold set, an extra pod is started. Currently the main bottleneck is the database, meaning the application itself does not experience a load that actually instantiates new pods.

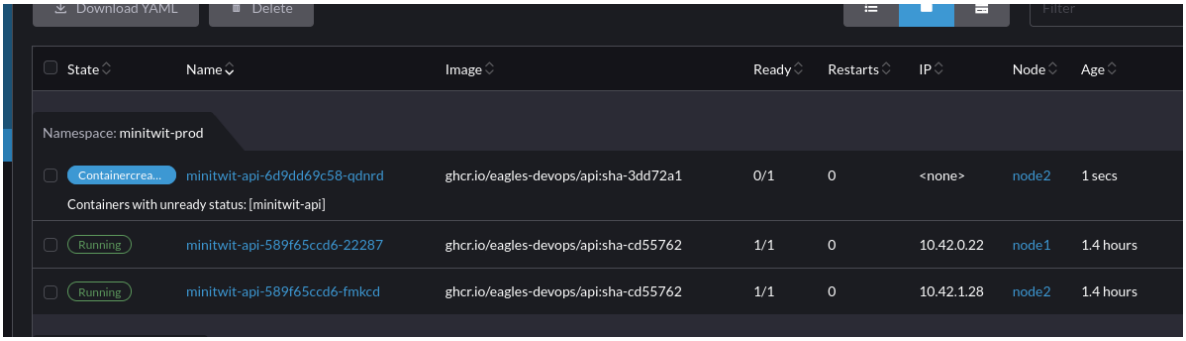


Figure 7: bluegreen

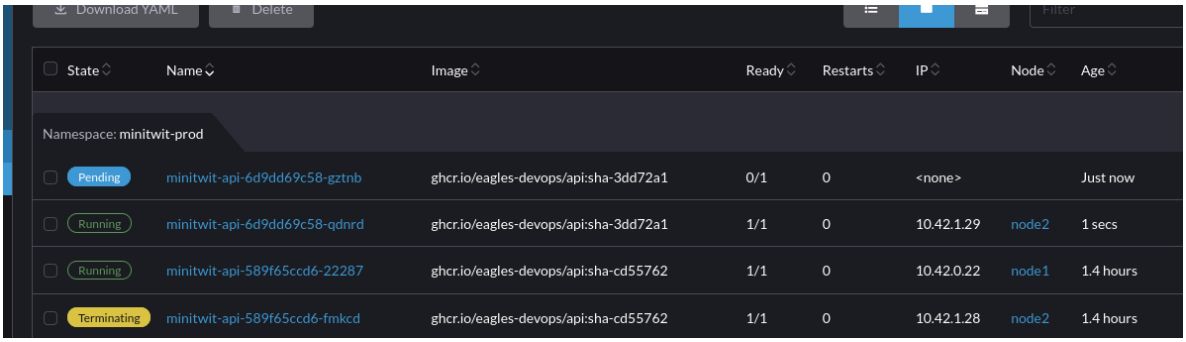


Figure 8: bluegreen

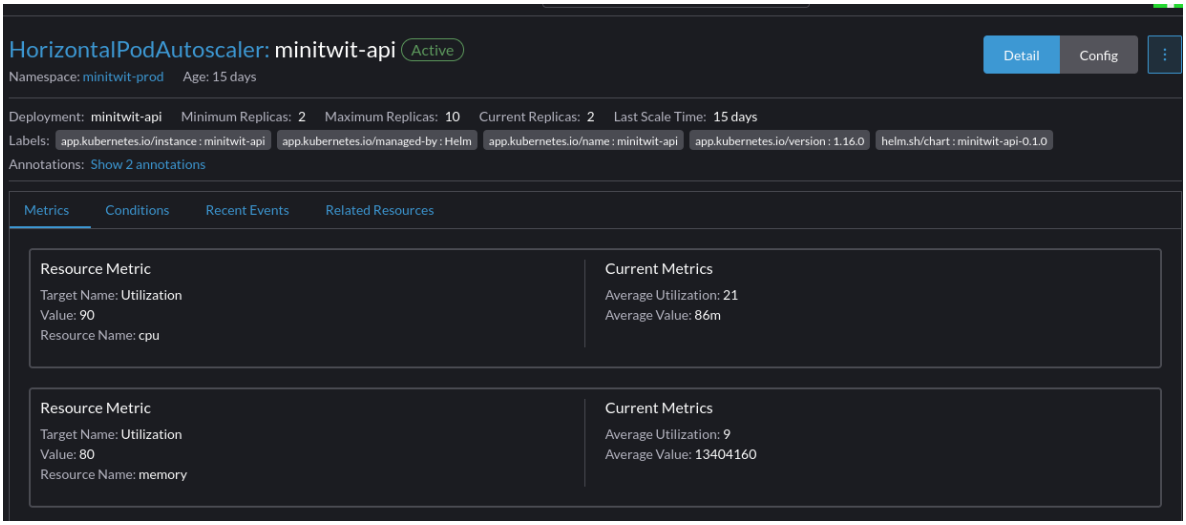


Figure 9: bluegreen

However by adding artificial stress on the cpu the autoscaling can be demonstrated:

Figure 10: bluegreen

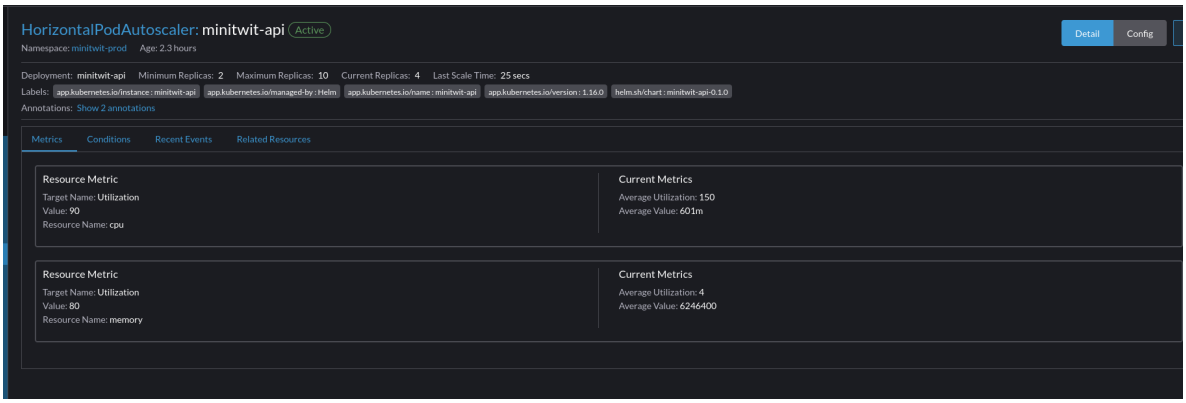


Figure 11: bluegreen

State of the system

This section will break down the current state of the system looking through multiple components and their current status. Such approach allows us to provide sufficient report and locate which sections of the project require more work. Before, lets show some general data about the application to get an idea of the traffic. MiniTwit application has processed **14,5 million** request during its up-time with somewhere above 1 million of reported errors. This makes 6% error rate.

Code Quality Analysis

SonarQube and CodeClimate were used to determine our code quality. Based on the last provided analysis from SonarQube our code seems to be secure with no security concerns. in terms of reliability, the code is proven to have a stable code base where most of the issues are related to other datetime variable interpretation than SonarQube is advising to use. Maintainability sections show the most issues with 87 recorded. Our code has a lot of error print statements which can be changed into constants. This would make the maintability part of the code much easier.
To summarize; our code base would appreciate some minor adjustments but none of the aforementioned concerns create potential harm to the codes stablity and readability.

Dependency scan

The project utilizes 100 dependencies based on the dependency report made by Snyk where there are 3 dependencies currently vulnerable to SQl injection. GitHub dependency report shows only 63 dependencies reporting similar issue regarding SQL injection vulnerability in some of the dependencies.

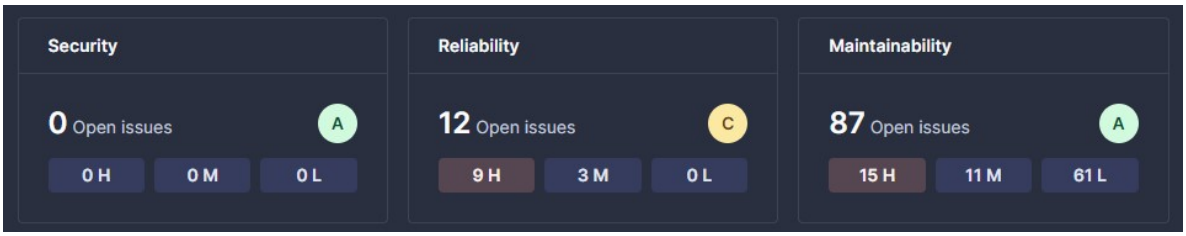


Figure 12: SonarQube general stats

GitHubs *dependabot* created PR with needed update of the vulnerable dependencies which should resolve the issues when merged into main.

Security Analysis

Static code analysis already showed us code quality when it comes to security point of view. In this field our projects shows good score. The application does not expose any vulnerable secrets which can be used to access any parts of the system. Our vulnerable information such as login details, SSH keys and other information are stored either in GitHub secrets or we have an .env file which each of members of the group store on their local machine. Sharing such sensitive information between developer is done via USB drive or sharing them through BitWarden. Moreoever, when potential problems occur, GitHubs Advanced Security bot will create an alert and block the open PR.

Test coverage

Application has a different sets of test - end-to-end, simulator tests, API tests as well as linters. Even with these tests in place we do not achieve 100% code coverage and some errors may slip through. Before every merge into main we did manual tests as well to catch bugs or other errors by hand. This method is not suitable in the long run. In the future, projects would require some time into making more test cases as well as different focus test sets.

Metrics, Logs and Dashboards

Application has monitoring running on Grafana utilizing Loki and Mimir as the data sources. Monitoring an application can be a huge project itself when done properly and in detail. Currently our application monitors the basic data which we were using to estimate the application performance. We can divide the data into 2 sections. First one is focus on more technical parameters which help the developers to asses the current errors or any other potential problems. Main monitored factors: failed requests, request duration, database read/writes. Second section are data related to business which can be easily understood by non-tech person. This includes number of users registered, amout of requests, number of messages and overall appliation status.

Application and all of its functionalities work as expected also under higher load of upcomming requests to the server. Application uptime was satisfactory except one major outage happening from *25/03 01:30* till *28/03 20:30* caused by a memory issue error on the VM and was not spotted for few days. In a real life scenario such outage would be unacceptable and should trigger alerts and other security tools to inform the developers about downtime.

Dependencies

Name	Description	Link
Golang	Statically typed, compiled high-level programming language	https://go.dev/
crypto	Package supplying different cryptography libraries for golang	https://golang.org/x/crypto
net/http	Package used to make HTTP requests	https://pkg.go.dev/net/http
Gorm	easy to use ORM library for Golang	https://gorm.io/gorm
Grafana	Open source analytics and monitoring solution used for database	https://grafana.com/
Mimir	long term storage for grafana data	https://grafana.com/oss/mimir/
Loki	Loki is a horizontally scalable, highly available	https://grafana.com/oss/loki/
Prometheus	open-source software for monitoring webapps	https://github.com/prometheus/
xxhash	Golang implementation of the (fast) 64-bit xxHash algorithm	https://github.com/cespare/xxhash
Gorilla	Package that supplies different tools for developing web-applications in golang	https://github.com/gorilla
Gorilla/mux	Package for request routing	https://github.com/gorilla/mux
Docker	System for deployment, containerized applications and development	https://www.docker.com/
Kubernetes	open source system for automating deployment, scaling, and management of containerized applications.	https://kubernetes.io/
Rancher	open-source multi-cluster orchestration platform	https://www.rancher.com/
Letsencrypt	free, automated, and open certificate authority used for SSL certificates.	https://letsencrypt.org/
zap	Package for fast logging in golang	https://github.com/uber-go/zap
SonarQube	open-source platform developed by SonarSource for continuous inspection of code quality	https://www.sonarsource.com/
Codeclimate	system that helps incorporating fully-configurable static analysis and test coverage data into a development workflow.	https://codeclimate.com/
pgx	PostgreSQL driver with toolkit for GO.	https://github.com/jackc/pgx/v5
pq	postgres for Go's database package	https://github.com/lib/pq
go-sqlite3	sqlite3 driver for Golang	https://github.com/mattn/go-sqlite3
Logs	Visualize an entire stack, aggregate all logs into structured data, and query everything like a single database with SQL.	https://betterstack.com/logs

2. Process' perspective

CI-CD

PR tests

A complete description of stages and tools included in the CI/CD chains, including deployment and release of your systems.

When code changes related to an issue are ready to be merged in to main, a pull request is opened, and unit- and integration tests are then run as a GitHub Action. These - along with a review, and passing the quality gate of the static analysis tool, are a prerequisit for the pull request to be completed.

Deployment

When the pull request is completed, the changed are merged to main triggering the ci-cd workflow. - Build docker image - Push docker image to registry - Deploy to K3S with Helm

Other workflow

We have a few other workflows as part of our setup.

As required a workflow generating a PDF top the report directory has been created.

A manually triggered workflow for running linters exists in linters.yaml.

Lastly a workflow for automating a weekly release is running at the end of each week. At this point it would make more sense to consider each automated deploy a release instead, but the automated release can be seen as a weekly snapshot.

AI chat bots

AI tools such as ChatGPT, Gemini, Opus-3 were used during the development stage. These tools were useful in many different cases. Usage helped us solve the errors much faster by providing us with clarity of the error messages. Another benefits such as code refactoring, topic explanation, and providing us with new approaches/tool to implement for the given problem. Usage of LLMs sped up the work and saved us a lot fo time.

Logging

How do you monitor your systems and what precicely do you monitor?

For monitoring we use Prometheus with Grafana. We do so by incrementing gauges or vectors whenever an event has succesfully occured In the system we monitor a multitude of things, for business data we log:

- We monitor the amount of users getting created.
- The amount of new followers on the platform
- Amount of new messages posted
- The total amount of reads and writes made to the database between releases.
- Besides incrementing counters we also monitor back-end data:
- The amount of failed database read-writes
- Whether there is a connection to the database
- Succesful HTTP requests

Monitoring these gives us an insight to the extend of traffic passing through our API. For ease of access to the monitored data and for visualization, the group uses Grafanas dashboards.

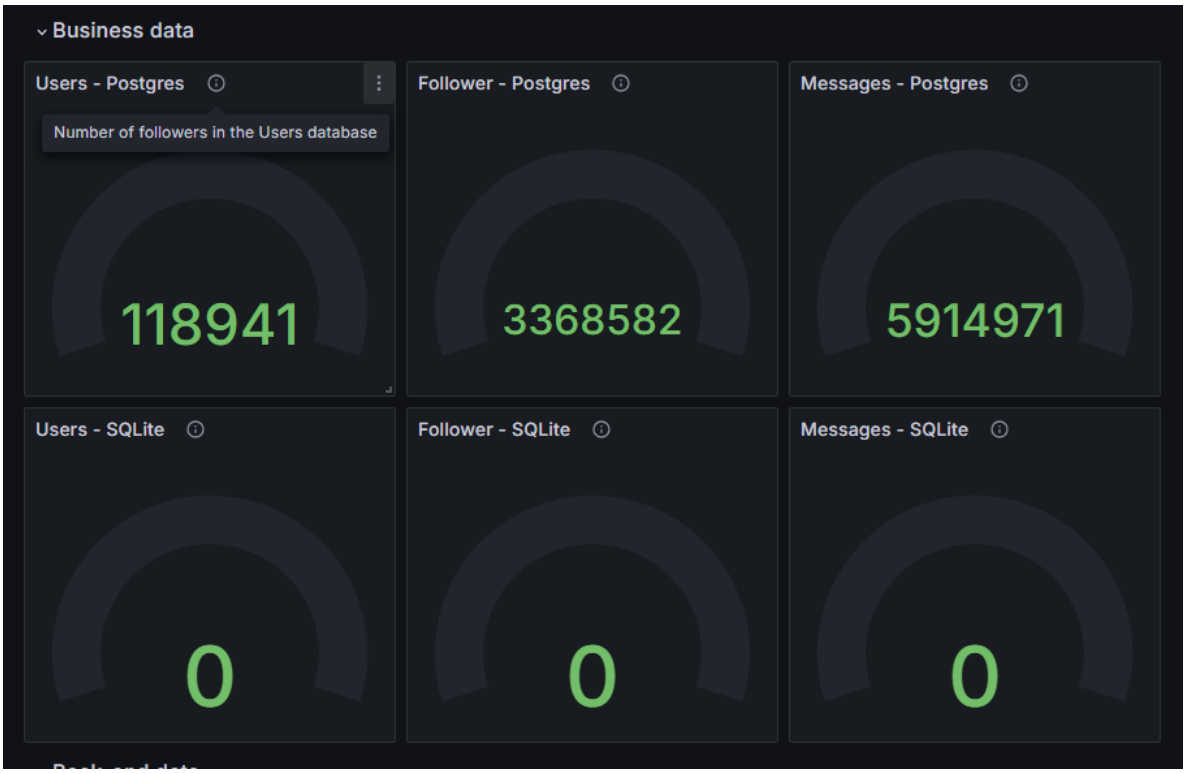


Figure 13: Grafana Business data monitoring

What do you log in your systems and how do you aggregate logs?

We log every error that happens during any database request. we log an info message each time some request happens.

This enables us to trace all the steps made through the API to (partially) rebuild the database in case of loss of data. We log every error that happens during any database request.

These are written through *zap*. The setup is such that the individual error logs are collected by logtail. Logtail then sends it to a Loki database that handles aggregation of the logs. The logs are visible through the Grafana Dashboard

It is important to note that we, due to time constraints, did not migrate our logs when moving to Kubernetes. The old logs and any new logs are hosted on the old production droplet.

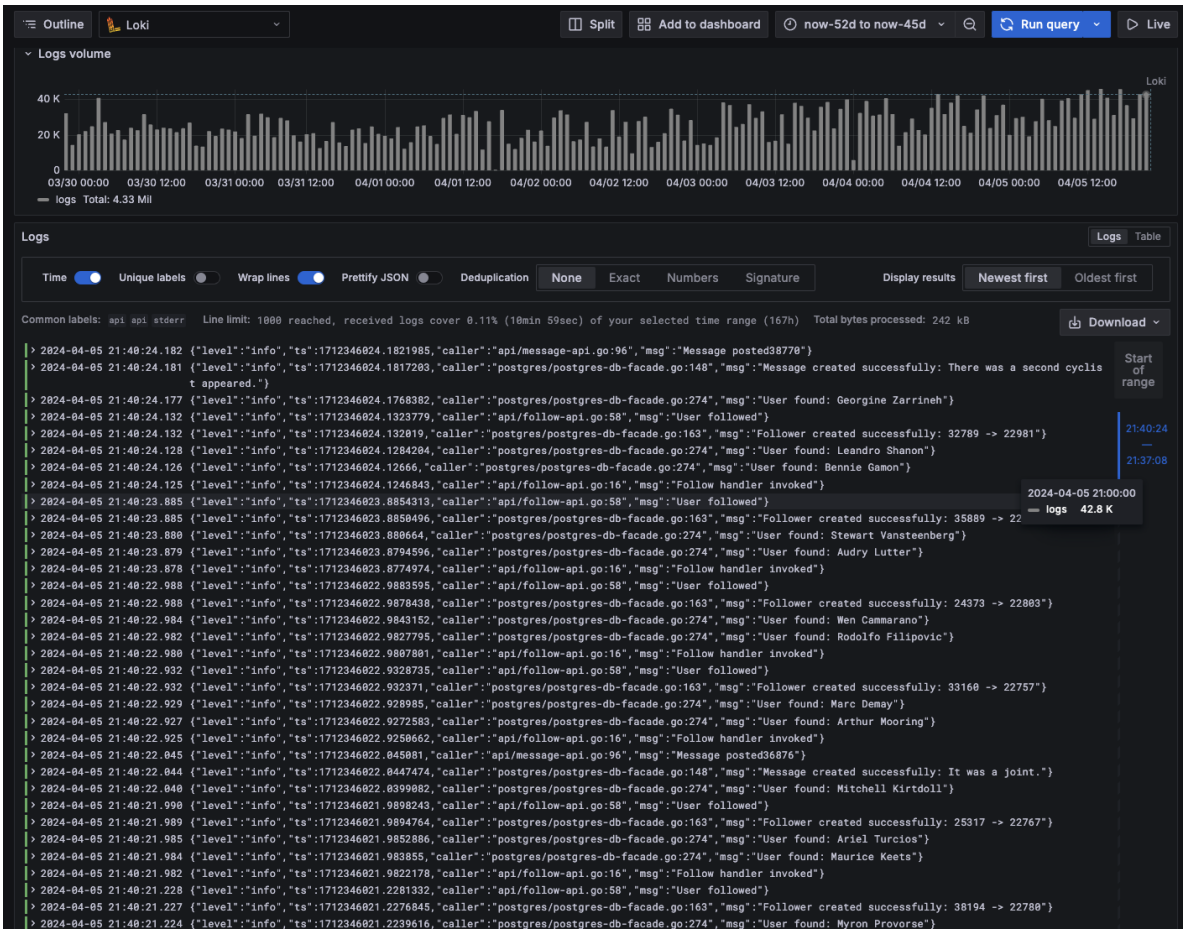


Figure 14: Info logs

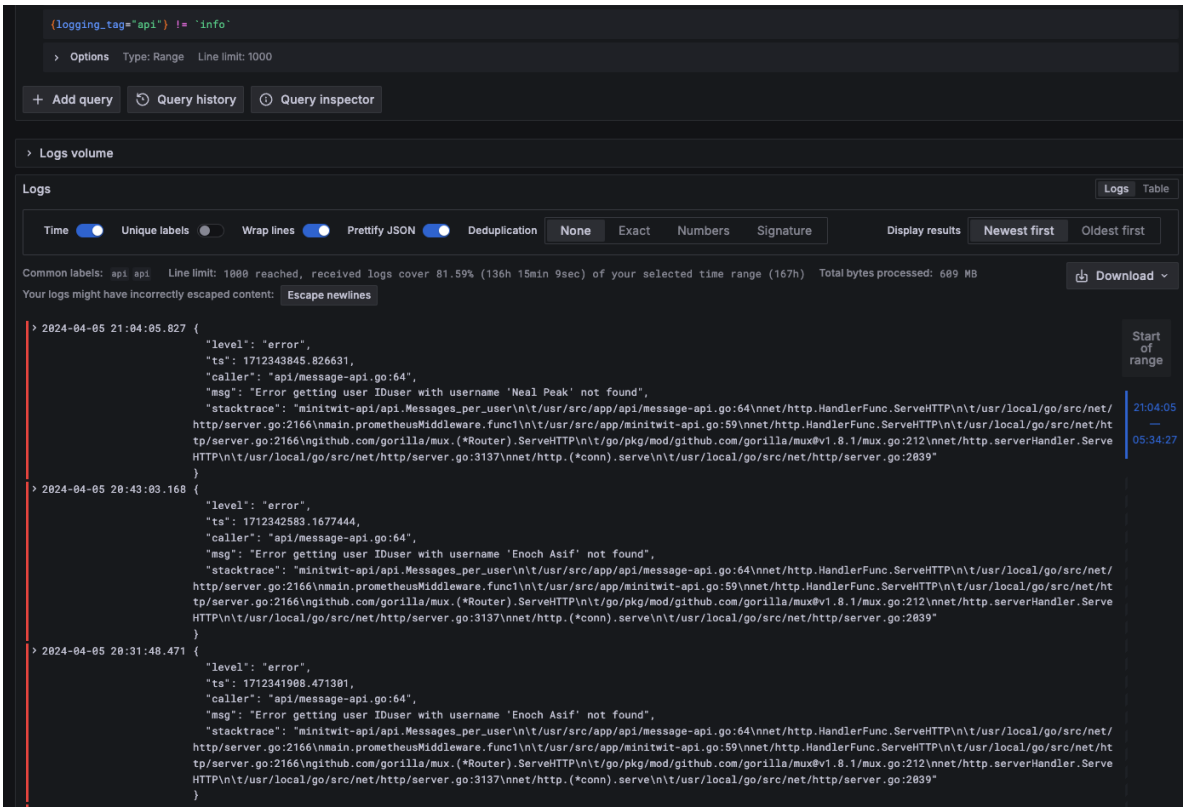


Figure 15: error logs

4. Lessons learned

Biggest Issues

In the initial stages of the development, whole team was working on refactoring the old code into new one. This created multiple instances of merge conflicts, different coding approaches. Furthermore the group could have spend more time on dividing big tasks into smaller tasks, as to minimize merge conflicts and large pull requests. With each group member having varying schedules, knowledge sharing fast was at times an issue, but this was resolved by planning joint meetings between either the parties that held the knowledge and the ones who needed it, or with the entire group. ## Reflection In the initial stages of the project, the group had some difficulties finding eachother within the team. After multiple conflict-resolution meetings improvements were made // Delete this line if you think it's bad (i do) After a while we managed to get a good communication flow and organized planning. Team members took tasks which they felt comfortable with but also wanted to gain new knowledge and improve. Code reviews were taken seriously which helped us to improve and reflect on the code before it was pushed into the main. Breaking down tasks and setting deadlines for them helped us to keep the whole project on track.

Techology choices

Programming Language

- **Choice:** GO
- **Considered:** Java, C#
- Lower memory consumption compared to ruby, Java etc.
- Scales well, which is important for us considering the userbase will increase over time.
- Easy to learn.
- Compiles to a single binary which makes it easy to deploy (compared to).
- Comes with an opinionated formatter (gofmt) ensuring code style consistency. This reduces discussions about styling (which does not bring value to the product).
- It is a language with high developer interest meaning that it will hopefully be ease future recruitment when the application sky-rockets in popularity.

Software Artifacts

- **Choice:** Docker
- **Considered:** VMs, Linux Packages, LXC, Go Packages
- Lower overhead compared to VMs.
- Supported on most Linux distributions regardless of package managers.
- Containers isolate the environment from the host system.
- Support for using different language compared to language specific artifacts.
- Support micro-services in our case allow us to run API and app with Docker Compose.
- Community support.

CI/CD Pipelines Tool

- **Choice:** GitHub Actions
- **Considered:** Jenkins, GitLab CI/CD, Bamboo
- Already integrated into code repository of our choice (Github).
- Minimal setup, compared to tools such as Jenkins.
- Runs on cloud without need of provisioning.
- Modern and easy to use UI.

Artifact Registry

- **Choice:** GitHub Container Registry
- **Considered:** DockerHub, GitHub Packages
- Largest docker registry.
- When using DockerHub we were only able to use an individual DockerHub account unless we were willing to pay for an organization. We chose GitHub Container Registry since it allowed us to publish container images directly in the GitHub organization. It also did not require us to use PATs since we could use the GITHUB_TOKEN from the action itself.

Infrastructure Automation Platforms

- **Choice:** Terraform
- **Previously Used:** Vagrant
- There is currently larger community behind Terraform than Vagrant.
- Less unexpected behavior we experienced compared to using Vagrant.

5. Conclusion

MiniTwit web applciation has performed with satisfactory results. All parts of the systems have been stable and functional during the whole development stage. The team has created an effective way of deployment and coordination which played a significant role towards the app performance. The application has encountered only one major downtime issue and besides this there were no other major problems, error have been envountered which could affect the state. (i don't quite understand the final sentence after the comma.)

6. References

7. Appendix

1. Dependency scan made with Snyk. Tested voth API app and Web app.

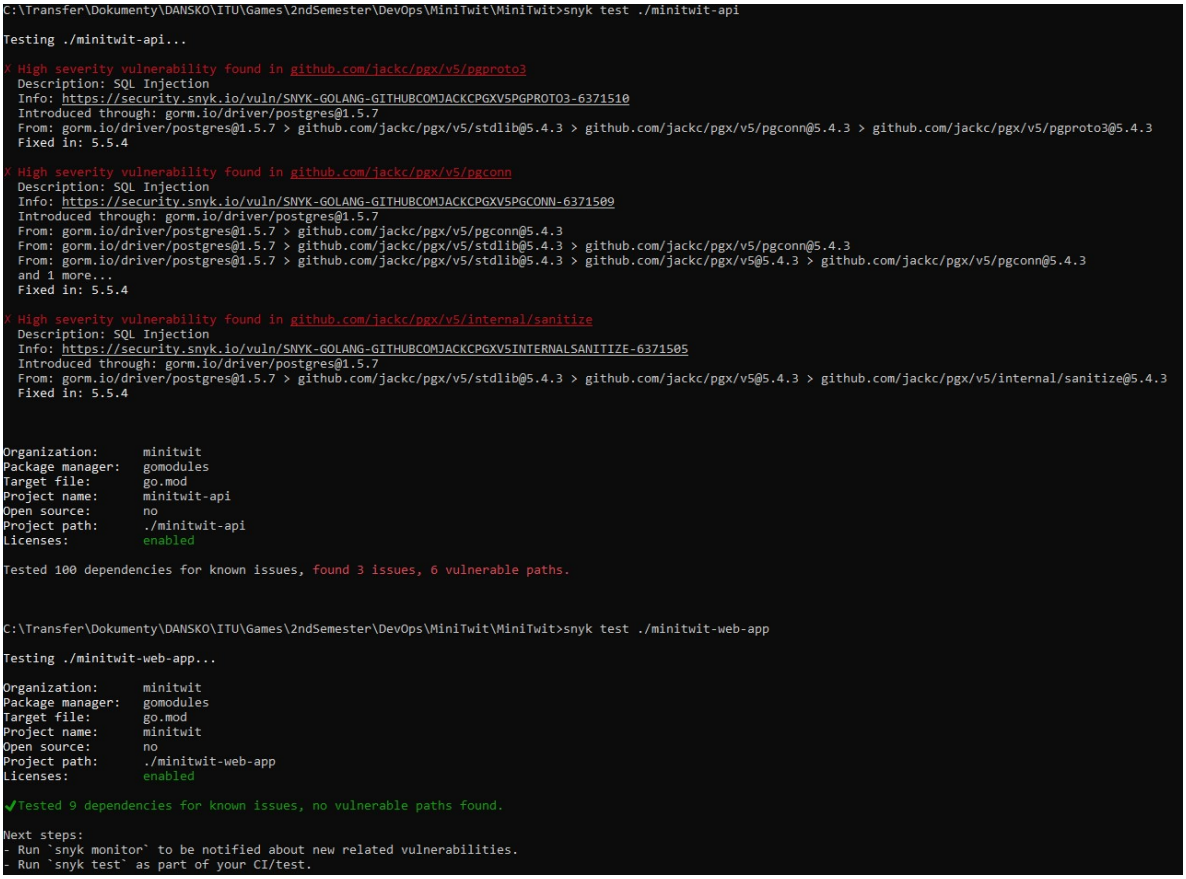


Figure 16: Dependency scan