DevOps 2025

IT University of Copenhagen

Team Sad People

People

- *Gábor Tódor* - gato@itu.dk
- *Kálny Zalán* - zaka@itu.dk
- *Nicklas Koch Rasmussen* - nicra@itu.dk
- *Nicolai Grymer* - ngry@itu.dk
- *Sebastian Andersen* - seaa@itu.dk

Subject

- **School:** *IT-University of Copenhagen*
- **Course manager:** *Helge Pfeiffer* - ropf@itu.dk
- **Course Code:** KSDSESM1KU

Introduction

System

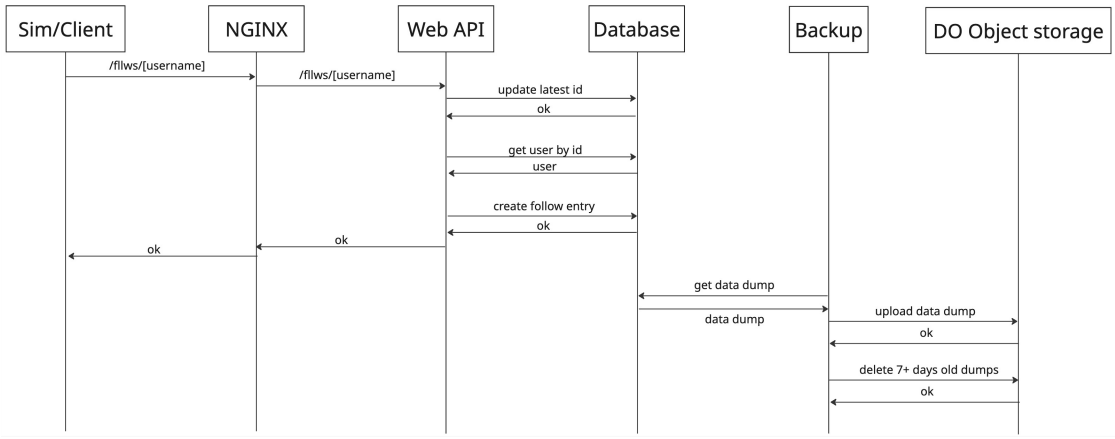
A description and illustration of the:

[seb/nick] Design and architecture of your *ITU-MiniTwit* systems

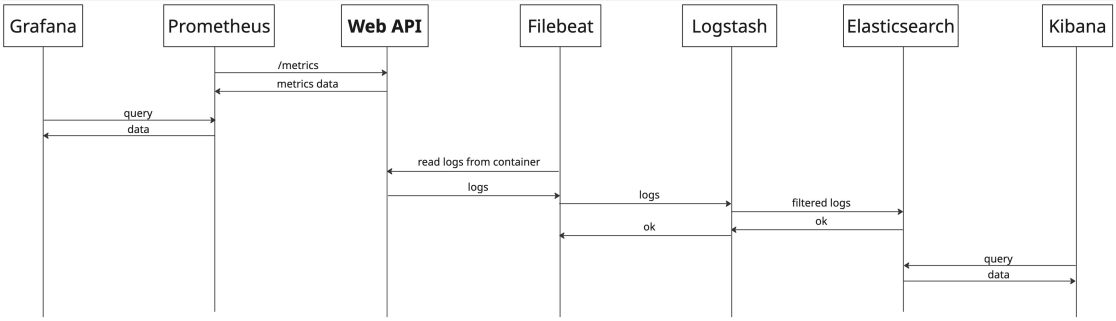
[Nic] All dependencies of your *ITU-MiniTwit* systems on all levels of abstraction and development stages. That is, list and briefly describe all technologies and tools you applied and depend on.

[Nic] Important interactions of subsystems.

Both the simulator and client contact the same API application, so both sequence diagrams look identical. The following sequence diagram uses the simulator request endpoint `/fllws/[username]` as the baseline. The following sequence diagrams does not take Docker Swarm into account, as the underlying communication is hidden.



For monitoring and logging, we have also included a sequence diagram to show how they interact with each other.



[G] Describe the current state of your systems, for example using results of static analysis and quality assessments.

[ALL] MSc students should argue for the choice of technologies and decisions for at least all cases for which we asked you to do so in the tasks at the end of each session.

Process

This perspective should clarify how code or other artifacts come from idea into the running system and everything that happens on the way.

In particular, the following descriptions should be included:

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

In the following section, we will discuss the CI/CD pipeline of our system, and for this, we discuss two key branches: `main` and `develop`. The `main` branch includes the code running on our production environment, and `develop` branch includes the code running on our staging environment. For the sake of communication, we will simply address these branches by `production` and `staging`.

We use GitHub for handling our repository and tracking the process with their issue system. We use a branching strategy, where features written in issues are worked on in `feature`-branches. Once ready, they are then merged into `staging` and then into `production`. This enables us to test and deploy the feature before production, at the cost of slightly longer delivery times. This means that for features to make it through to production, it includes three phases:

1. We work on the issue using a `feature`-branch. Developers work on and finalize the feature on this branch.
2. Once ready, a pull-request is created to merge the `feature`-branch into `staging`, where tests, linting, static code analysis and a fellow team member, must pass or approve the request, before being able to merge it into staging.
3. Once deployed to the staging environment, if the staging environment sees no failures and passes a manual test, a pull-request into `production` is made. Once approved by tests, linting, static code analysis and a fellow team member, the feature is pushed into main.

Automated Testing and Quality Gates

Pull-requests as well as pushing to staging and production, include several tests that are performed using workflows that trigger a GitHub action, which builds a Docker container with which these tests can be performed. On top of the web API container, an associated PostgreSQL database is instantiated, to perform E2E and simulation tests.

- Unit tests are performed using Ruby Rack
- E2E tests are performed using Playwright
- Simulation tests are performed by instantiating a new environment, and using Python to perform requests
- Static code analysis using SonarQube, which requires ≤3.0% code duplication in the Ruby application.

GitHub branch protection rules ensure that developers follow this workflow. Concretely it prevents users from merging directly into the `staging` and `production` branch.

On top of the above, Ruby and Docker code is formatted and linted on push to any branch. This is done using the GitHub action modules `standardrb/standard-ruby-action@v1` and `hadolint/hadolint` respectively.

Build and Deployment Process

We deploy using GitHub Actions, which builds containers and uploads them to Digital Ocean's container registry. We also upload a new version of the Ruby application, and if there are updates to the configs for either our monitoring or logging stack, we also push a new version of that. If tests pass, then we automatically continue to deploy. Currently we differentiate between containers designated for the staging and production environment by assigning them such a tag.

The deployment process involves SSH'ing into the manager node of the Docker Swarm, that is running as droplets (virtual machines) on Digital Ocean, and running a deploy.sh script, which simply pulls the newest version of the stack from the container registry.

On pushes to main, we automatically create a new release, which includes bumping the application with a new minor-update, meaning 1.0.0 turns into 1.1.0. If we wish to introduce a patch or major update, we can specify in the commit message.

We orchestrate the containers using Docker Swarm, and given the size of our application, we currently follow the direct deployment rollout strategy, where we simply push a new version to all worker nodes at once. This is a point for improvement.

Environment Management and Infrastructure

We have manually set up instances using Digital Ocean's interface, but have prepared a Terraform script for setting up a new environment in the future. For artifact management, we use Digital Ocean's container registry, where we only differentiate between container versions using staging and production tags.

To distribute secrets that GitHub Actions can access, we set up GitHub secrets to keep an access key to Digital Ocean on which we deploy our application.

Rollback Strategy

To roll back, it would require manually SSH'ing into the server and modifying the compose script to depend on a specific container in Digital Ocean's registry. This is definitely a weak point, making it time consuming to rollback and represents an area for future improvement.

Monitoring and Observability

Once the feature is successfully integrated into the production codebase, we use Prometheus and Grafana to monitor the application, ensuring that the feature introduces no error, and that operation levels remain the same. In case of noticeable changes, we use Kibana to navigate logs to help diagnose the problem. Kibana queries Elasticsearch, which receives logs from Logstash, who in turn accesses log-files using Filebeat.

[Z/G] How do you monitor your systems and what precisely do you monitor?

[Z/G] What do you log in your systems and how do you aggregate logs?

[Nic] Brief results of the security assessment and brief description of how did you harden the security of your system based on the analysis.

By running through the OWASP Top 10 list on security assessment, we have done the following analysis:

- A01:2021-Broken Access Control In the system only two levels of access control exist in the system. Either you are a user, who can post, follow and unfollow, or you access as a public user. For user-specific endpoints, we have not found any vulnerabilities. CORS settings however, allow anyone to access the API. This misconfiguration allows malicious websites to make authenticated requests to the API on behalf of logged-in users.
- A02:2021-Cryptographic We've upgraded from HTTP to HTTPS, but still expose the port of the application, meaning IP:PORT still gives users access to the service in non-encrypted ways, such that

network eavesdroppers can capture username and passwords. The hashing algorithm has been upgraded from MD5 to SHA256, but unfortunately without salting, allowing attackers who gain access to the database to easily crack passwords with rainbow tables or brute force attacks. Lastly, the simulator protection-key is hard-coded which means anyone with access to the public github repo, can essentially bypass that security measure.

- A03:2021-Injection We use the ORM Ruby Sequel, which includes sanitization of input before constructing SQL statements. Developers can create raw SQL statements, but we have opted not to do this given the impracticality and security risks.

A04:2021-Insecure Design Given the tiny feature set, we could not find anything particularly noteworthy about the design.

A05:2021-Security Misconfiguration After experiencing a ransomware attack, requiring bitcoin for our data, we closed ports and changed the default password to prevent future attacks. Similarly, we discovered that `ufw` was disabled by the end of the course, which exposes all services to the web. Lastly, we are aware that CORS settings are overly permissive as elaborated in A01.

A06:2021-Vulnerable and Outdated Components Our system has very weak password checking, which allow users to create easily hackable accounts. Simultaneously, weak email validation and not sending a confirmation email makes it particularly easy for bots to create users. In fact, 99.9% of our activity is from a single bot.

On the developers side, we did not require 2FA to log into DigitalOcean, bringing our level of security down to the weakest login-type of the five team members. And technically, Dependabot has been suggesting a Ruby update from `3.3.7` to `3.4.4`, which have been postponed multiple times.

A08:2021-Software and Data Integrity We have not been able to identify any issues regarding this.

A09:2021-Security Logging and Monitoring Failures We experienced a log overflow causing our production service to fail. This failure did not cause any warnings, causing three days of downtime for our application. We will elaobrate on how we fixed this when reflecting on system operation.

A10:2021-Server-Side Request Forgery We have not been able to identify any issues regarding this.

[Seb/Nick] Applied strategy for scaling and upgrades.

[Nic] In case you have used AI-assistants during your project briefly explain which system(s) you used during the project and reflect how it supported or hindered your process.

This project included the use of both chatbots and in-editor help using copilot. These were provided by OpenAI and Anthrophic.

Copilot increased speed by solving minor problems through it's line-for-line help. To increase the precision, prompt-like comments would be added prior to the line of interest, or specific prompts would be used to concretely specify the desired change.

Chatbots on the other hand involved four primary types of prompts:

- Elaboration: Please explain X technology
- Comparing: What is the difference between X and Y technology
- Creation: I want to X
- Solving: I want X, but instead Y happens.

Elaboration and comparison were primarily used at the planning stage of implementing new technologies, or for developers unfamiliar with existing technologies already implemented.

Creation is used throughout the implementation of technologies or features, but the scale of the issues attempting to address diminishes over time, as the feature or technology becomes more intergrated into the system, and required changes are smaller. As more code is added to the codebase, solving unwanted behavior becomes more important, and makes out large parts of prompts.

Additional reflection on use of chatbots, we found that Claude 3.7 Sonnet provided better code-based responses as well as understanding misconfigurations and bugs. It gives detailed descriptions of different variables and potential flaws in the code and configs. This is measured against ChatGPT o1.

Reflection

Evolution and refactoring

Finishing a sprint and adding a new feature

[G/Z] ELK logging resource heavy + too many fields + all fields were indexed

[G/Z] Filebeat on all swarm nodes

[G/Z] Logging deployment: put config images in

[Nic] Database migrating from SQLite to PostgreSQL to PostgreSQL

The migration from SQLite to Postgresql happened at a stage, where no active users was using our platform (The simulator was yet to start). This meant that we could safely upgrade without having to move over data, which would have otherwise been a hassle given the SQL dissimilarities.

Given the educational purpose of the project, we later sought out an opportunity to perform a database migration. Such an opportunity arose when database optimization became a necessity. Before optimizing, we deemed it necessary to introduce an ORM, which would improve the developer experience as well as migration experience going forward. Given the new database structure introduced by the ORM, although quite similar, we needed to migrate from one database with one schema, to another database with another schema. The approach taken involved extracting data from one postgres instance in the shape of SQL Insertion statement, which we then manipulated to fit the new data scheme, and then simply ran the sql insertion statements in the new database.

As soon as the migration was done, we switched to the new application image, meaning we now served requests from the new database. This approach involved having 5 minutes of forgotten data, and 3 seconds of lost availability. We found this price and strategy reasonable, although the 5 minutes of lost data, could have

had serious impact on the business. As we will later discuss, we found that using logical replication, proved to be a much nicer approach to copying data.

[Nic] Transition from docker compose to docker swarm (networking problems).

Transitioning onto multiple machines with docker swarm came with multiple obstacles. First, the docker compose version running on certain of the docker compose scripts, were unsupported by docker swarm. WRITE HERE, WRITE HERE **[Seb/Nick] Docker compose versioning problem (moving to stack)**.

Second, the swarm nodes were able to communicate with each other, but self-instantiated virtual networks defined in the docker-compose file, did not propagate to worker nodes, leaving application containers unable to contact the database, and prometheus unable to collect monitoring events. To accommodate the issue, we destroyed and redeployed new virtual machines, and this time used the VPC IP address to define the IP address of the manager node. This meant that workers are referring to the manager using the virtual network layer, and solved the communication issue.

[G/Z] scp files onto server and then deployment (Discuss ups/downs)

```
- You can destroy the prod environment with wrong files/wrong docker compose
```

[G/Z] Transition from config files to docker images (Tagging docker containers)

[Seb/Nick] Large amount of features cloging up in staging (Impossible to migrate to production)

Operation

Keep the system running

[Nic] Database logical replication resulting in db crash

Migrating from docker compose to the docker swarm included the use of postgres feature: Logical replication, which allows postgres instances to live sync data from running postgres instance to the other. This feature is typically used to keep a hot stand-in database ready. In our case, it meant we would actively sync data from the active production database, onto the new production database, and allow us to switch from one stack to the other with zero downtime, as the stand-in database would become the new default.

Unfortunately, after switching a few days later, the pub/sub mechanism of logical replication in Postgres accidentally corrupted a tracking file, meaning the postgres would immediately crash on start. This problem was accomodated by immediately running `pg_resetwal` on startup to reset the corrputed file, and then unsubscriping from the expired subscription. The subscription does not provide any value at this point, as we swapped from the old to the new production machine, and the old one has been turned off.

[G/Z]Log overflow problem. Access denied to machine. Massive clutch

[Nic] Backup strategy (cron job every three hours)

Although it's great to solve problems on yuor own, sometimes other have done a great job already. And this proved to be the case for backing up a Postgres database. Simply adding the `eeshugerman/postgres-backup-s3:15` container image to the manager node and configuring environment variables, we successfully setup a cron job that automatically backs up daily, and sends the backup to DO's space storage, which is S3 compatible. Using the exact same script, it also includes functions that easily allow restoring from a previous backup. The latter is a crucial step, for when things are burning. The container likewise provide clean-up functionality, such that only 7 days of backups are kept.

Maintenance

Keep system up to date and fix bugs

[Seb/Nick] Stale ReadMe.md throughout project

[Seb/Nick]Returning wrong statuscode (Misalignment with simulation)

- Thanks to running similator in the CI/CD pipeline we found this

[Nic] Upgrading to NGINX, setting up ufw, moving to domain

Upgrading to NGINX, we learned multiple things about running a system. First being that having a staging environment to learn how to run command in the correct order proved great to build a shell script that immediately upgrades the production service. Second, that although we had configured our ufw with all the right ports, actually the service was disabled, which it is by default. Only by realizing that the 443 port was open although no specified, did we realize that ufw needs to be actively activated. From this we gathered, that it is important to double check firewall and other security measures, to ensure they're configured properly. Luckily, our database was not exposed by PORT from the docker network, and therefore inaccessible, but having full access to other ports may have exposed other vulnerabilities on the machine.

[Nic] Simulator IP protection stopped sim access (causing errors)

Refactoring simulator requests to only be accepted from a single IP address helped us prevent other malicious users from interfering with the active simulation requests. However, when the new update was pushed, unfortunately the IP protection feature also protected us from the actual simulation IP. Although this worked perfect locally, moving it onto production showed that the feature declined all sim api requests. From this we learned about the importance of being able to quickly roll back an update. During this experience, we found that we did not have a previous versioned container ready to roll back to, and instead had to allow all IP's which was possibly by passing in `ACCEPTED_IPS=*`, which essentially disabled the IP protection.

Style of work

Reflect and describe what was the "DevOps" style of your work.

[Seb/Nick] Reflect on the workflow. Extensive Friday meeting. Split work into three groups

[Seb/Nick] Development environemnt: local => branch => staging => production

[Seb/Nick] Repo settings. Workflows on merge. Require 1 team member on pull requests.

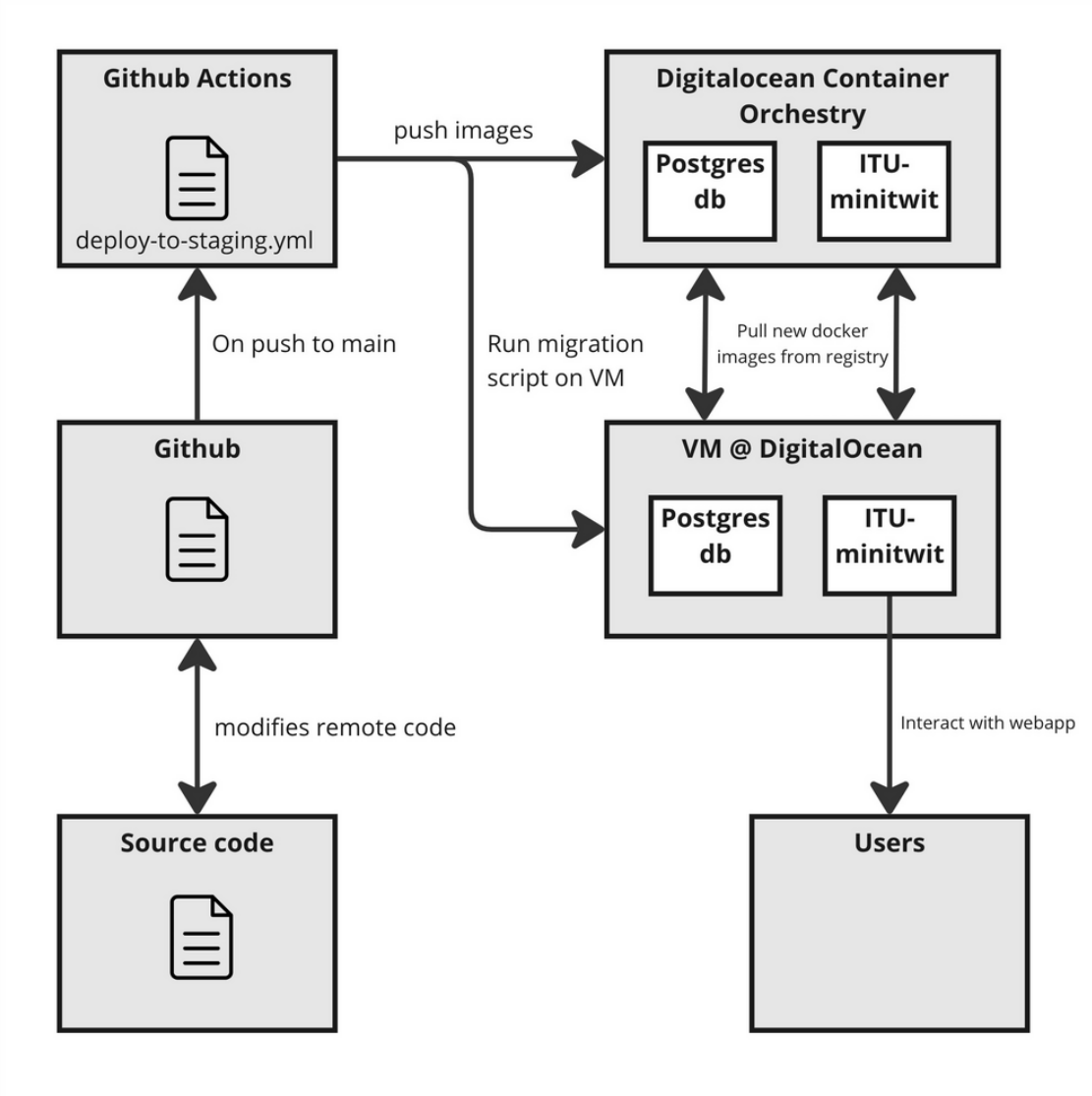
[Seb/Nick] Running simulator in workflows

That's it folks!

REMEMBER TO REMOVE THIS

THIS IS JUST AN EXAMPLE

THIS IS JUST AN EXAMPLE



hello a LOL fdsa