High Performance and Cloud Basic assignment: Cloud-Based File Storage System

Stefano Cattonar

Course of AA 2023-2024 - Data Science and Artificial Intelligence

1 Problem statement

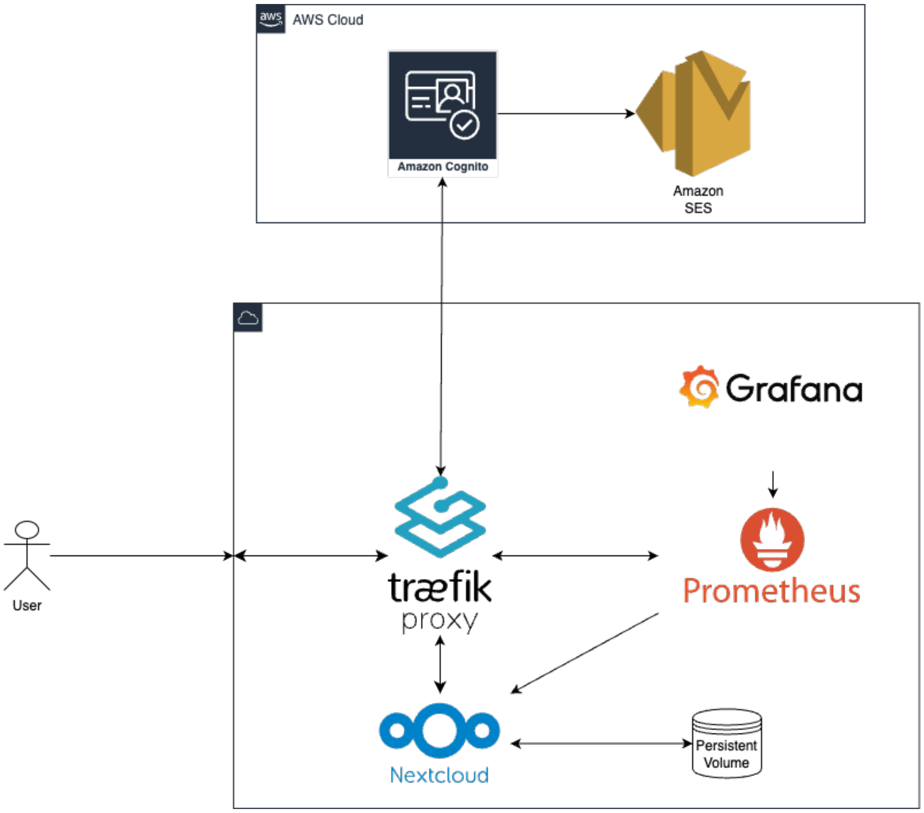
The purpose of this project is to design a Cloud-Based File Storage System. During the assignment, the student should design an architecture with the following characteristics:

- Users should be able to sign up, log in, and log out and should have their private space
- Users should be able to upload, download and delete files to their private storage
- The design should support different roles (e.g., regular user and admin) and a role should have the ability to manage regular users

And it's important to adress the solution security, scalability and cost-efficiency

2 Proposed Architecture

The solution I designed for this assignment is the following:



The components of this system are:

- Traefik is a reverse proxy and load balancer (MIT license)
- Prometheus collects metrics from configured targets at given intervals, evaluates rule expressions, displays the results, and can trigger alerts when specified conditions are observed. (Apache 2.0 license)
- Grafana allows you to query, visualize, alert on and understand your metrics no matter where they are stored (AGPL-3.0 license)
- AWS Cognito is a Customer identity and access management (CIAM) and an OAuth2 and SAML Identity Provider (closed source and distribuited as SaaS)

- Nextcloud is an expandible, open-source, self-hosted file synchronization and sharing plat-form designed to provide secure, private, and customizable cloud storage solu-tions for individuals and organizations. (AGPL-3.0 license)

As you can see, it's a combination of different software, many of which are free open source, but where the FOSS solution was too expensive to implement, I decided to use a SaaS(AWS Cognito and AWS SES) because when you are creating a solution it's important to focus on which product can give you the best cost-effectiveness.

2.1 Traefik

We use Traefik as the only entrypoint of our architecture thanks to it's reverse proxy capabilities. This give us a few advantage in security:

- Attackers can't directly call the others services
- We can add and remove headers from request and response
- Traefik can manage SSL certificates for domains and sub domains

2.2 Prometheus

Prometheus is used as metrics scraper and data source for Grafana. It role it's to collect metrics from all the others services(except for AWS Cognito) to sodisfy one of three pillars of observability. It's possibile to use Prometheus to do query on it's data and to make automatic alerting from them.

2.3 Grafana

In this solutions Grafana is used to visualize all the metrics scraped by Prometheus in convinient dashboard accessable by admins to monitoring the entire system perfomance.

2.4 AWS Cognito

AWS Cognito is a Software as a service (SaaS) made by Amazon Web Servises for costumer identity and access management. In this solution, it's used as OAuth2 identity provider to give us a software indipendent way to manage users. The costs for AWS Cognito are really low and it's free tier cover until firfty thousand monthly users.

2.5 Nextcloud

Nextcloud is the core of this solution. It's a expandable open-source storage system, designed as alternative to iCloud, One Drive and similar solutions from public cloud providers. I installed the extension to use OAuth2 authentication.

2.6 What is missed?

- A tool (or more than one) to scrape logs and traces, to follow all of three observability pillars(Grafana Loki + Grafana Tempo, or OpenTelemetry for example.

- One Secret Management software like Hashicorp Vault, because put secrets (as token or password) inside git repository is a really security hole. Put secrets inside docker swarm secrets is an "okay" solution, but on kubernetes not because secrets are just the base64 version of the original text.

- A way to make more resiliant the NextCloud filesystem, for example integrating it with AWS S3 or Garage, to have copies on different availability zones or regions.

3 Deployment

For this exercise I prepared a docker compose and a script that is needed for some setup, expecially in the NextCloud server. You will find all the instruction in the readme.md inside the public GitHub repository