Logcraft

Lucas JAROSSON - Tristan COMBAZ - Maxime BACON

Contexte

Dans une petite entreprise de 25 employés spécialisée dans la gestion de documents juridiques, l'infrastructure informatique est externalisée auprès d'une société de services en informatique (SSII).

Parmi les services déployés en interne, un serveur Nextcloud auto-hébergé permet aux collaborateurs de stocker, partager et collaborer sur les documents sensibles de l'entreprise.

Cependant, après un incident mineur lié à la perte temporaire de fichiers partagés, le responsable de la sécurité de la SSII constate que le serveur Nextcloud ne dispose pas d'un système de journalisation centralisée.

Expression du besoin

- Se mettre à niveau par rapport à la doc ANSSI
- Avoir une base de données pour stocker les journaux,
- Avoir un système permettant de centraliser et visualiser les logs générés.

Objectif du projet

Les objectifs du projets sont ：

- Mettre en place un serveur centralisé pour les logs.
- Les enregistrer dans une base de données via rsyslog
- Consulter les logs sur l’appli

Fonctions principales

- Stocker les logs dans une base de données.
- Déploiement d’un serveur web.
- Conception d’une application web.
- Mise en place d’un dashboard pour consulter les logs.

Critères de performances

- Les logs doivent être accessibles, triés et complets.
- Sécurité (chiffrement des données, MAJ régulière et sauvegarde)
- Intégrité des données

Contraintes technique

- Utilisation de deux VM (ubuntu) en IPV6
- Développement PHP (version 8) orienté objet
- Limitation lié au réseau (blocage firewall)
- Récupération des données via rsyslog

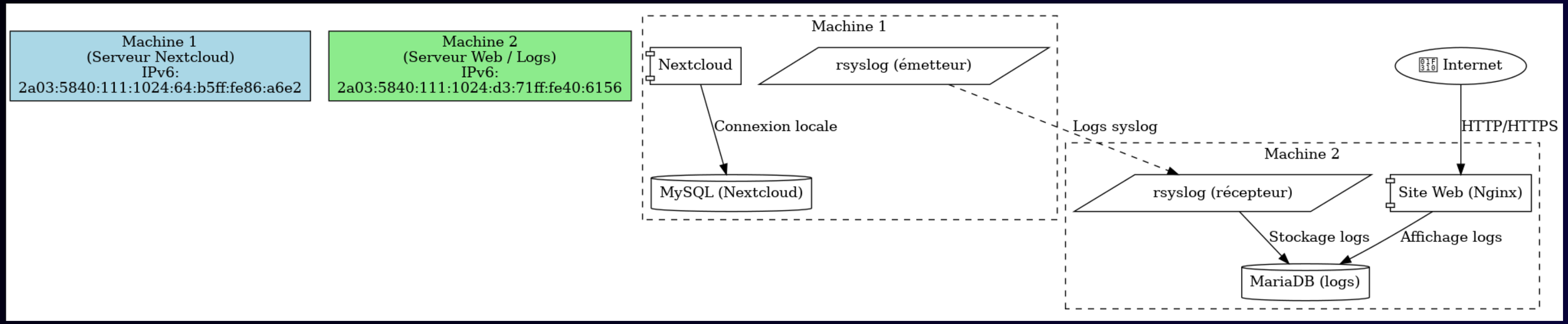
Répartition des tâches

Lucas	Diagram de classes / cas d'utilisation	Installation /conf de la mariadb	Installation de rsyslog	Installation / Configuration Nginx	Développement du site web	Analyse statique	35%
Tristan	Création des deux instances	Installation/configuration nextcloud	Création plan réseau	Configuration du rsyslog	Installation et configuration serveur NTP	Explication infra pour création documents	35%
Maxime	Reco doc ANSSI	Diapo	Documents				30%

Matériel et logiciels utilisés

- 2 Machines Virtuelles Ubuntu.
- Docker & Docker Compose.
- MariaDB.
- Rsyslog.
- Nginx avec PHP(version 8), tailwinds

Plan réseau


Machine 1
(Serveur Nextcloud)
IPv6:
2a03:5840:111:1024:64:b5ff:fe86:a6e2
Machine 2
(Serveur Web / Logs)
IPv6:
2a03:5840:111:1024:d3:71ff:fe40:6156
Machine 1
Nextcloud
rsyslog (émetteur)
Connexion locale
MySQL (Nextcloud)
Logs syslog
Internet
HTTP/HTTPS
Machine 2
rsyslog (récepteur)
Site Web (Nginx)
Stockage logs
Affichage logs
MariaDB (logs)

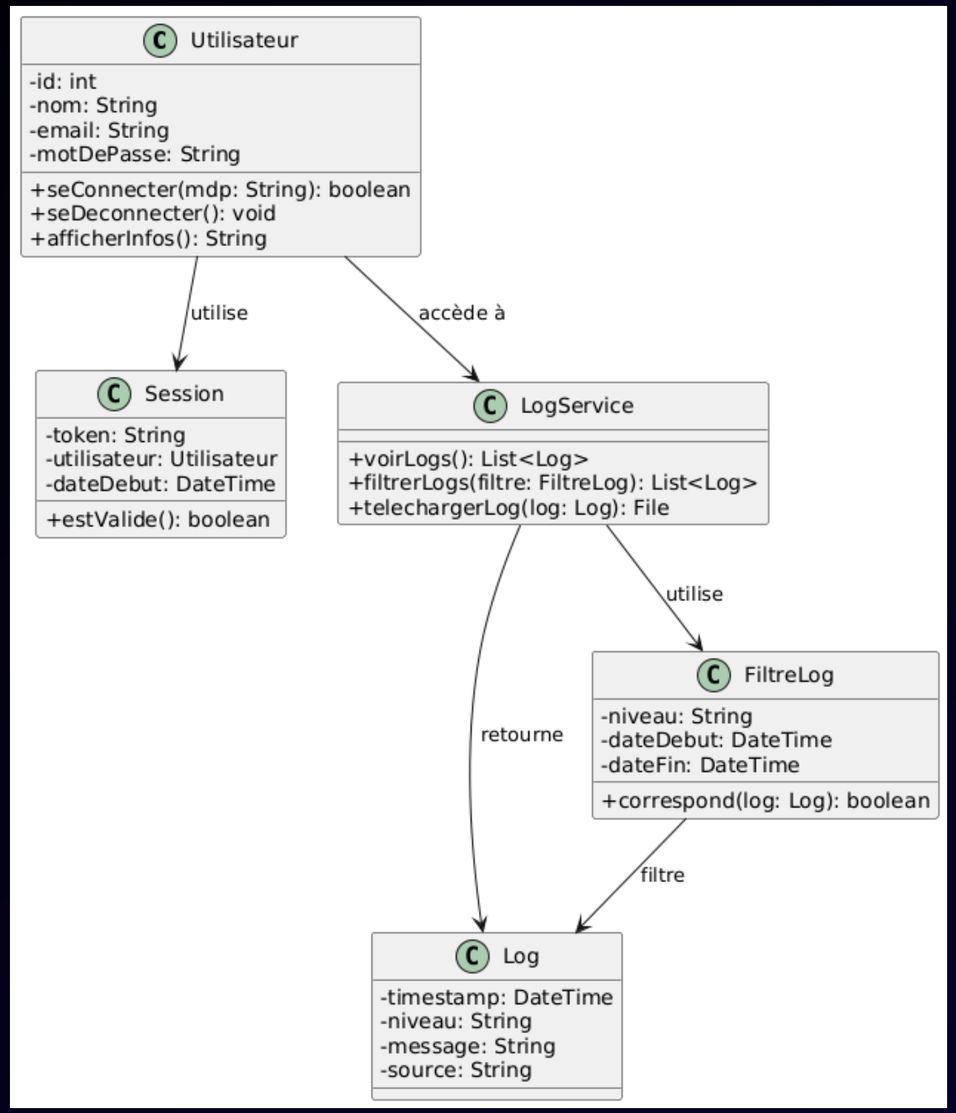
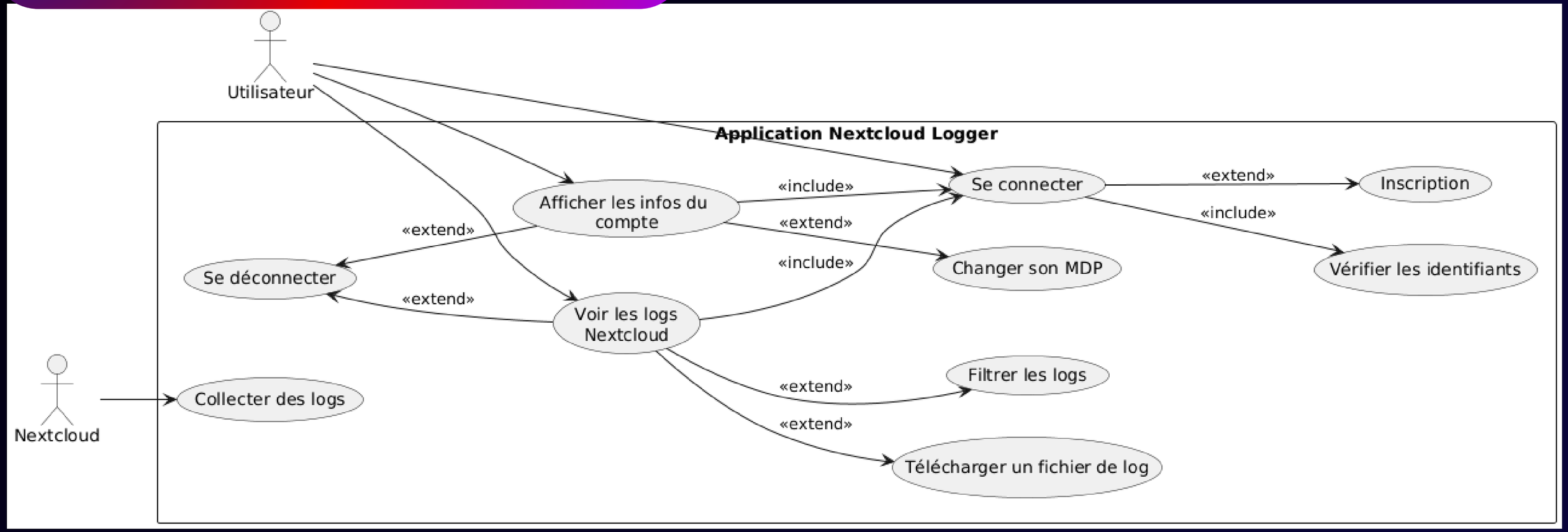


Diagramme de classe

Diagramme Use Case



Livrables attendus

- Base de données avec logs stockés via rsyslog
- Documentation technique
- Application de restitution des logs

Tests de validation

- Connexion à l’application
- Affichage des toutes les logs Nextcloud
- Filtrage des logs
- Affichage des logs par utilisateurs et par actions

Merci

Lucas JAROSSON - Tristan COMBAZ - Maxime BACON