// Rapport de projet technique — BTS SIO option SISR

Infrastructure cloud privée supervisée

Nextcloud, reverse proxy sécurisé et supervision — VMware / Ubuntu Server

Auteur : Sahed Arshed Ali Khan

Formation : BTS SIO — option SISR, CFA Aurlom

Période : 2025

Environnement : VMware Workstation, Ubuntu Server

NEXTCLOUD NGINX / SSL-TLS ZABBIX FAIL2BAN MFA / TOTP

01. Contexte & objectifs

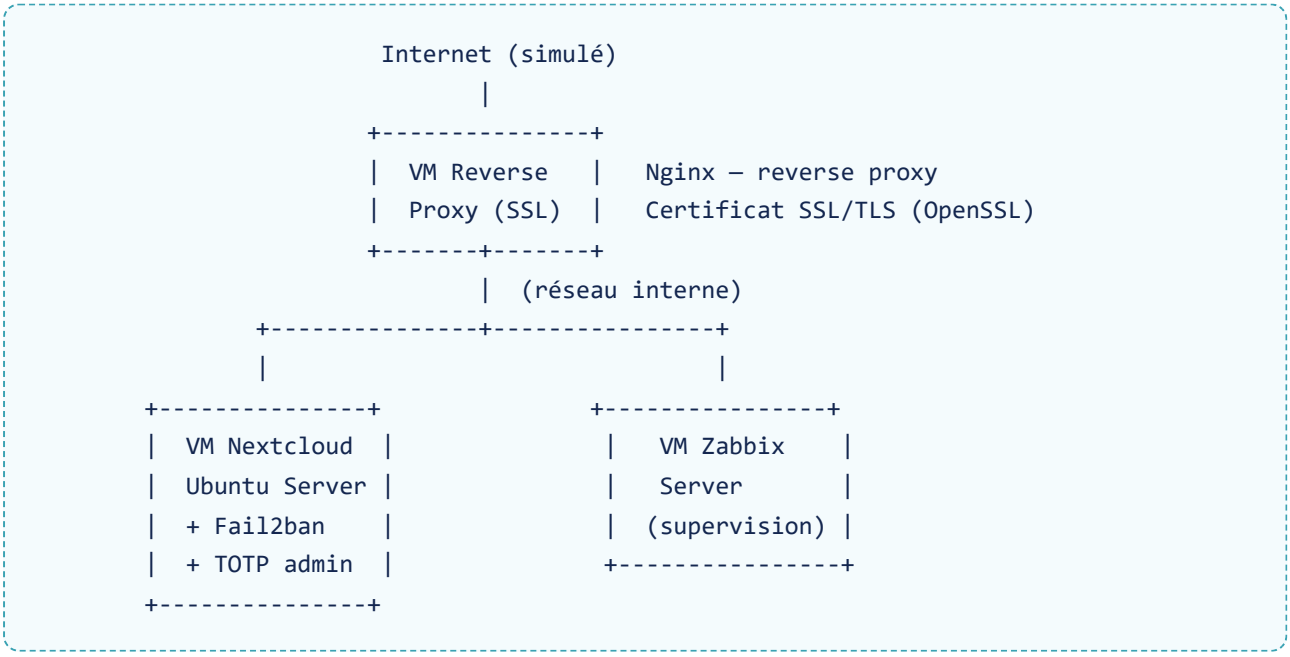
De nombreuses petites structures hébergent leurs documents sur des services cloud tiers, avec un contrôle limité sur la localisation et la sécurité des données. Ce projet reconstitue la mise en place d'un **cloud privé** auto-hébergé, permettant à une organisation de garder la maîtrise complète de ses données tout en offrant une expérience de partage de fichiers comparable aux solutions grand public.

Au-delà du simple hébergement, l'enjeu technique portait sur la sécurisation de bout en bout de l'accès (chiffrement, authentification renforcée, protection contre les attaques par force brute) et sur la capacité à détecter rapidement un incident grâce à la supervision.

> **OBJECTIFS TECHNIQUES VISÉS**
>
> Déploiement d'une plateforme Nextcloud multi-VM · chiffrement des échanges (reverse proxy Nginx + SSL/TLS) · authentification à deux facteurs (TOTP) · durcissement contre le brute-force (Fail2ban) · supervision de la disponibilité (Zabbix).

02. Architecture retenue

L'infrastructure repose sur plusieurs machines virtuelles VMware, chacune dédiée à un rôle précis afin de limiter la surface d'exposition de chaque composant et de faciliter la supervision indépendante des services.



VM	RÔLE	OS	ADRESSE (RÉSEAU INTERNE)
vm-proxy	Reverse proxy / terminaison SSL	Ubuntu Server LTS	10.10.0.10
vm-nextcloud	Application Nextcloud + Fail2ban	Ubuntu Server LTS	10.10.0.20
vm-zabbix	Supervision (server + interface web)	Ubuntu Server LTS	10.10.0.30

03. Réalisation

Déploiement de Nextcloud

Installation de Nextcloud sur une VM Ubuntu Server dédiée (pile LAMP), configuration du stockage des données utilisateurs et création des comptes avec des quotas définis.

Reverse proxy et chiffrement

Mise en place d'un reverse proxy Nginx en frontal, générant et appliquant un certificat SSL/TLS afin que tous les échanges entre les utilisateurs et la plateforme soient chiffrés (HTTPS uniquement, redirection forcée depuis HTTP).

Authentification renforcée

Activation de l'authentification à deux facteurs (TOTP) pour les comptes à privilèges, réduisant fortement le risque de compromission par simple vol de mot de passe.

Durcissement contre les attaques

Configuration de Fail2ban avec une règle (« jail ») dédiée à Nextcloud, bannissant automatiquement toute adresse IP multipliant les échecs d'authentification sur une courte période.

Supervision

Déploiement d'un serveur Zabbix avec agents installés sur chaque VM, définition de déclencheurs (triggers) sur la disponibilité du service Nextcloud, l'espace disque et la charge système, avec remontée d'alertes en cas d'anomalie.

04. Tests & validation

- **Chiffrement :** vérification du certificat SSL/TLS et du refus des connexions en clair (redirection HTTP → HTTPS effective).

- **MFA :** test de connexion avec un compte protégé par TOTP — accès refusé sans le second facteur.
- **Anti brute-force :** simulation de tentatives de connexion répétées échouées — bannissement automatique de l'IP par Fail2ban confirmé dans les logs.
- **Supervision :** arrêt volontaire du service Nextcloud — remontée d'une alerte Zabbix dans le délai attendu.
- **Disponibilité :** tests de montée en charge légers (upload/download simultanés) pour vérifier la stabilité du reverse proxy.

05. Conclusion

Ce projet a permis d'aborder la sécurisation d'un service exposé de bout en bout : chiffrement des échanges, authentification renforcée, protection contre les attaques automatisées et supervision proactive. Il illustre concrètement la démarche de durcissement (« hardening ») qu'un administrateur systèmes et réseaux doit appliquer avant la mise en production d'un service.

> **COMPÉTENCES BTS SIO – SISR MOBILISÉES**
>
> Administration Linux (Ubuntu Server) · déploiement et configuration d'un reverse proxy · gestion de certificats SSL/TLS · authentification multi-facteurs · durcissement de service (Fail2ban) · supervision applicative (Zabbix).

Document rédigé dans le cadre du portfolio de synthèse — BTS SIO, option SISR. Projet réalisé en environnement de virtualisation VMware.