Manuel dÉxploitation et de Continuité dÁctivité
Infrastructure, Sauvegardes et Workflow

Équipe Technique Skills Hub

Janvier 2026

Table des matières

1 Introduction

Ce document présente lárchitecture technique de la plateforme Skills Hub du BUT TC, ainsi que les procédures critiques pour garantir la disponibilité et líntégrité des données pédagogiques.

2 Infrastructure des Serveurs

La solution repose sur une séparation stricte entre les environnements.

2.1 Serveur de Production

— **URL :** `https://home.educ-ai.fr`
— **Ports :** 80 (HTTP), 443 (HTTPS).
— **Rôle :** Utilisation réelle par les étudiants et le staff.

2.2 Serveur de Développement

— **URL :** `https://dev.educ-ai.fr` (via port 8081)
— **Commande :** `npm run dev:start`
— **Rôle :** Bac à sable pour tester de nouvelles fonctionnalités sans impact sur la production.

3 Stratégie de Sauvegarde

Le système de sauvegarde est conçu pour parer à une perte de données majeure ou une corruption.

3.1 Stockage Externe (4 To)

Les sauvegardes sont exportées chaque nuit sur le serveur `tc-portail` :
— **IP :** 172.16.95.98
— **Partition dédiée :** `/srv/tc-data/backups`
— **Rétention :** 1825 jours (5 ans).

3.2 Automatisation

Le script `infrastructure/backup_production.sh` est exécuté à 3h00 du matin via `cron`. Il effectue :

1. Le dump SQL des 4 bases (App, Keycloak, Odoo, Mattermost).
2. La copie physique du dossier `uploads` (Preuves et Portfolios).
3. La compression et le transfert via `rsync` par clé SSH.

4 Scénarios de Crise et Remise en Service

4.1 Scénario A : Erreur humaine (Suppression accidentelle)

Symptôme : Un étudiant a effacé son portfolio ou une base a été corrompue.

1. Identifier lárchive du jour précédent sur le serveur de 4 To.
2. Utiliser la commande : `npm run prod:restore backup_full_YYYY-MM-DD.tar.gz`.
3. Valider la restauration des données spécifiques.

4.2 Scénario B : Attaque par Ransomware (Cryptolocker)

Symptôme : Les fichiers sur le serveur de production sont cryptés et inaccessibles.

1. **Isolation :** Couper immédiatement le serveur de production.
2. **Réinitialisation :** Réinstaller le système déxploitation du serveur.
3. **Récupération :** Les archives sur le serveur de 4 To sont isolées (via SSH sur port non-standard 4660) et restent saines.
4. **Déploiement :** Cloner le dépôt Git, puis lancer `npm run prod:restore` avec la dernière archive saine.

4.3 Scénario C : Panne matérielle totale du serveur

Symptôme : Le serveur de production est hors-service physiquement.

1. Provisionner une nouvelle machine (VM ou Physique).
2. Installer Docker et Docker-Compose.
3. Récupérer la dernière sauvegarde depuis `172.16.95.98`.
4. Lancer `docker-compose up -d` et injecter les bases SQL.

5 Guide du Développeur

5.1 Workflow Git

— **Branche `main` :** Code stable uniquement. Chaque push déclenche une sauvegarde.
— **Branche `develop` :** Pour les nouvelles vues et corrections en cours.

5.2 Commandes Utiles

```
# Lancer l\'environnement de test (Port 8081)
npm run dev:start

# Verifier l\'etat des sauvegardes distantes
npm run prod:check-backup

# Effectuer une sauvegarde manuelle immediate
npm run prod:backup
```

6 Sécurité

— **Accès :** Láccès au serveur de backup se fait exclusivement par clé SSH RSA 4096 bits.
— **Mots de passe :** Aucun mot de passe nést stocké en clair dans les scripts.
— **Isolement :** Le serveur de backup nést pas accessible depuis lÍnternet public, uniquement via le réseau interne.