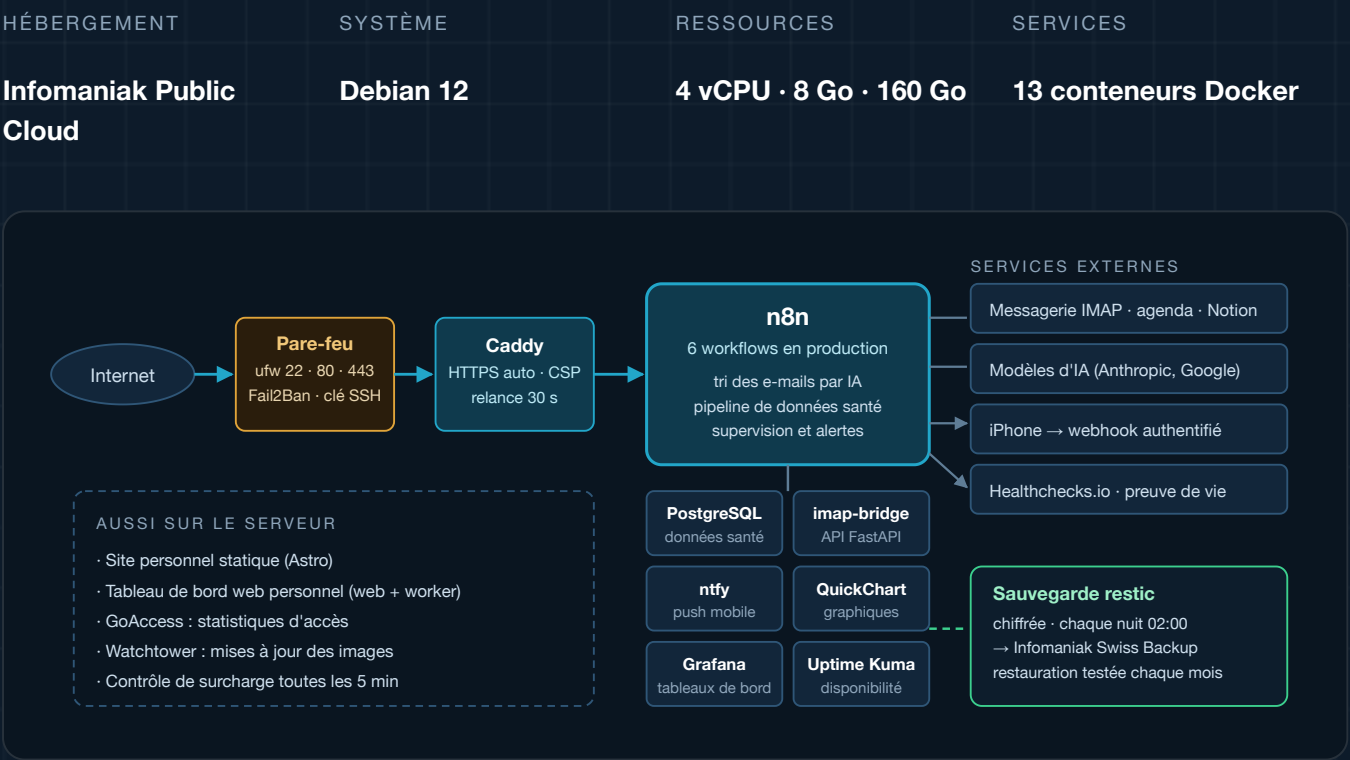


Serveur Linux auto-hébergé et automatisation n8n

Un serveur virtuel que j'administre de bout en bout : durcissement, services en conteneurs derrière un reverse proxy HTTPS, flux d'automatisation n8n reliés à la messagerie, à l'agenda et à des modèles d'IA, supervision avec alertes, sauvegardes chiffrées et restauration testée chaque mois.



6workflows n8n en production

5 minentre deux preuves de vie envoyées à Healthchecks.io

109instantanés de sauvegarde vérifiés, aucune erreur

1x/moisrestauration automatique testée (dernière : réussie)

Debian 12

Docker Compose

n8n

PostgreSQL

Python · FastAPI

API REST · webhooks

IMAP / SMTP

Caddy · HTTPS

ufw · Fail2Ban

restic

Grafana

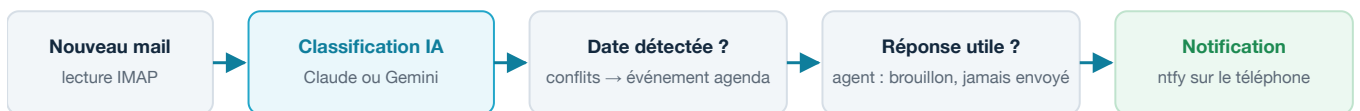
Uptime Kuma

01 Sécurité par couches

COUCHE	MESURE EN PLACE
Réseau	Pare-feu ufw qui refuse tout par défaut ; seuls SSH, HTTP et HTTPS sont ouverts. Les services applicatifs ne sont joignables que par le réseau Docker interne.
Accès	SSH par clé uniquement, mot de passe désactivé, connexion root interdite ; administration avec un compte non-root et sudo.
Attaques	Fail2Ban bannit une adresse après 3 échecs SSH ; les sous-réseaux récidivistes sont bloqués de façon permanente.
Web	HTTPS automatique (certificats obtenus et renouvelés par Caddy), politique de sécurité du contenu (CSP) par site, cookies sécurisés pour n8n.
Secrets	Identifiants des workflows chiffrés par n8n ; clé de chiffrement incluse dans les sauvegardes, clé restic conservée hors du serveur.

02 Workflows n8n en production

Tri de la boîte mail par IA



21 nœuds. L'agent de rédaction consulte l'agenda et Notion pour le contexte, mais ne fait que préparer un brouillon : l'envoi reste une décision humaine. Un petit service maison en Python (FastAPI) expose la messagerie aux workflows : recherche, lecture, brouillon, envoi.

Pipeline de données santé

Le téléphone envoie ses mesures à un webhook protégé ; n8n valide et aplatit les données, refuse les appels non autorisés (401), puis les insère dans PostgreSQL. Chaque lundi, un résumé hebdomadaire rédigé par IA et un graphique (QuickChart) arrivent sur le téléphone ; chaque jour, une détection d'anomalies alerte en cas de valeur inhabituelle. Grafana sert de tableau de bord.

Supervision et alertes

Les erreurs des workflows déclenchent un workflow d'erreur dédié qui m'envoie une notification. Toutes les 5 minutes, le serveur envoie une preuve de vie à Healthchecks.io : si elle s'arrête, l'alerte vient de l'extérieur, même si le serveur entier est tombé. Uptime Kuma surveille la disponibilité des sites.

03 Sauvegardes et reprise après sinistre

- **restic** chiffré, dédupliqué, vers le stockage Swiss Backup d'Infomaniak (hors du serveur), chaque nuit à 02:00.
- **Contenu** : export complet des bases PostgreSQL, copie cohérente de la base de n8n, tous les volumes Docker (dont la clé de chiffrement de n8n et les certificats), configurations système et projets.
- **Rétention** : 7 jours, 4 semaines, 6 mois, avec vérification d'intégrité du dépôt.
- **Restauration testée** automatiquement le 1^{er} de chaque mois : la base est restaurée et contrôlée, le résultat est signalé à Healthchecks.io.
- **Procédure de reprise** écrite pas à pas pour remonter le serveur sur une machine neuve.

```
# /etc/cron.d (extrait)
0 2 * * * root /root/backup.sh
0 5 1 * * root /root/restore-drill.sh

# journal de la nuit du 12.10.2026
check snapshots, trees and blobs
109 / 109 snapshots
no errors were found
=== backup OK ===

# test de restauration du 01.10.2026
OK: pg dump restored & valid
OK: n8n sqlite restored & integrity=ok
=== restore drill PASSED ===
```

04 Incidents détectés et corrigés

TÂCHES JAMAIS LANCÉES	En mettant en place les sauvegardes, j'ai découvert que le service cron n'avait jamais été installé : une ancienne tâche de sauvegarde locale n'avait donc jamais tourné, sans aucun message d'erreur. Installé et activé, puis chaque tâche critique a reçu sa preuve de vie externe. Leçon : une tâche planifiée n'existe que si quelqu'un vérifie qu'elle s'exécute.
ERREURS 502	Les mises à jour automatiques des conteneurs redémarrent n8n chaque semaine ; pendant ce temps, les appels entrants recevaient une erreur 502 et étaient perdus. Le reverse proxy patiente désormais jusqu'à 30 secondes et réessaie avant de répondre. Leçon : prévoir le redémarrage comme un cas normal.
BASE QUI GROSSIT	L'historique d'exécution de n8n est limité à 7 jours et 5 000 exécutions pour garder une base légère et des sauvegardes rapides.

05 Prochaines améliorations

Versions

Épingler les images critiques (n8n) au lieu de suivre « latest », et mettre à jour volontairement.

Workflows versionnés

Exporter les workflows n8n dans un dépôt Git pour suivre chaque modification.

Reproductible

Durcissement de base décrit en script pour monter un nouveau serveur en quelques minutes.