

n8n est une ai spécialisée : dans le cadre de mon mémoire licence3 / bachelor 3 pour un titre RNCP administrateur & système, dans mon approche je ne suis pas stagiaire mais un externe ayant deux tickets totalement différents. Je dois réaliser une mini audit technique pour comprendre les besoins et les failles puis sachant que les données sont centralisées via des consoles synology vers un serveur qui utilise trois box vers les serveurs d'infomaniak en suisse. Chaque synology est lié à un corps de métier bureautique / développement / contrat etc (je détaillerai plus tard). Une fibre noire sert de première réserve de backup. les transferts via les synologies sont immédiates pas de différés donc pas de pertes. Ma seconde mission déployer sur infomaniak une visioconférence device: jitsi pour tester son déploiement à moyen terme plus étendu que nuji qui utilise jitsi pour des meetings entre clients et juristes. Étendre via un loadbalancer l'usage de 1 à 5 / 5 à 15 / 15 à 50 puis 50 à 500 pour tester aussi le monitoring et la sécurité des données qui utilisent cette interface audio / vision / et partage de documents.

Je comprends votre contexte professionnel et vos deux missions principales. Permettez-moi de clarifier quelques points pour mieux vous accompagner :

Correction technique : n8n n'est pas une IA spécialisée, mais une plateforme d'automatisation workflow (comme Zapier) qui permet de connecter différents services et d'automatiser des tâches.

Analyse de votre infrastructure actuelle : Votre architecture semble suivre ce schéma : Synology (par métier) → 3 box → Serveurs Infomaniak (Suisse) + fibre noire en backup. Les synchronisations temps réel via Synology sont effectivement un point fort pour éviter les pertes de données.

Pour votre audit technique, je vous suggère de structurer votre approche autour de ces axes :

L'**analyse des flux de données** entre les différents Synology selon les métiers, l'**évaluation des points de défaillance** (les 3 box semblent être un goulet d'étranglement potentiel), et l'**analyse de la redondance** (fibre noire vs connexions principales).

Concernant Jitsi sur Infomaniak : Votre approche de montée en charge progressive (1→5→15→50→500) est judicieuse. Pour le load balancing, il faudra considérer la répartition géographique des serveurs Infomaniak et les spécificités de Jitsi (qui peut être gourmand en ressources).

Souhaitez-vous que je détaille l'un de ces aspects ou avez-vous des questions spécifiques sur la méthodologie d'audit ou l'architecture Jitsi ?

Clarification sur n8n :

n8n est un outil d'automatisation de workflows gratuit et open-source, pas une IA spécialisée. C'est une plateforme qui donne aux équipes techniques la flexibilité du code avec la rapidité du no-code, avec plus de 400 intégrations et des capacités IA natives.

Structuration de votre mémoire :

Mission 1 : Audit technique de l'infrastructure existante

Architecture actuelle à analyser :

- Synology par métier (bureautique, développement, contrats)
- 3 box (point critique à identifier)
- Serveurs Infomaniak Suisse
- Fibre noire en backup

Points d'audit prioritaires :

- Cartographie des flux de données entre métiers
- Analyse des goulots d'étranglement (les 3 box)
- Évaluation de la redondance et continuité de service
- Sécurité des transferts de données

Mission 2 : Déploiement Jitsi sur Infomaniak

Objectifs de montée en charge :

- Phase 1 : 1-5 utilisateurs
- Phase 2 : 5-15 utilisateurs
- Phase 3 : 15-50 utilisateurs
- Phase 4 : 50-500 utilisateurs

Éléments à tester :

- Performance du load balancer
- Monitoring système
- Sécurité audio/vidéo/partage documents
- Comparaison avec la solution actuelle (nujls)

Souhaitez-vous que je détaille la méthodologie d'audit ou l'architecture Jitsi en priorité ?

Autre point l'entreprise est soucieuse des risques (ancien hackeur, éthique actuellement) ils m'ont refusé : Nmap / Netsat / APR et lynx. J'ai ce document de base.

Analyse du document fourni :

Ce comparatif révèle une infrastructure hétérogène avec des **vulnérabilités significatives** identifiées :

Machines à risque critique :

- **APR-F-MEHDI, APR-F-STAGE, KUS-F-UGO** : CPU 7e génération (vulnérables Spectre/Meltdown), RAM insuffisante, BIOS anciens
- **APR-F-LOU** : GPU faible (512 Mo) limitant les capacités

Contraintes de sécurité de l'entreprise : L'interdiction de **Nmap, Netstat, ARP, Lynx** montre une politique de sécurité stricte. Ces restrictions compliquent l'audit réseau traditionnel mais sont compréhensibles vu le profil de l'entreprise.

Approche d'audit adaptée : Au lieu des outils interdits, vous pouvez utiliser :

- **Analyse passive** via logs système
- **Outils intégrés Windows** : ipconfig, ping, tracert
- **PowerShell** pour inventaire (sans scan actif)

- **Monitoring des performances** via Gestionnaire des tâches/Ressources

Questions pour préciser votre audit :

1. Ces machines sont-elles connectées aux Synology ou font-elles partie d'un autre segment ?
2. Avez-vous accès aux logs des Synology et des "3 box" ?
3. L'entreprise a-t-elle des outils de monitoring déjà en place ?

Recommandations prioritaires basées sur ce document :

- Segmentation réseau pour isoler les machines vulnérables
- Plan de remplacement des machines critiques
- Audit des configurations de sécurité sans outils intrusifs

Souhaitez-vous que je détaille une méthodologie d'audit "passive" adaptée à ces contraintes ?

En fait il y a trois catégories : ressources / fichiers / administratifs donc trois synology spécifiques avec trois box qui vont basculer via la console qui contrôle le switch la charge en fait ils font office de loadbalancer.

Clarification de l'architecture :

Maintenant je comprends mieux votre infrastructure :

Architecture logique :

3 Synology spécialisés :

- ├── Synology RESSOURCES (gestion des ressources)
- ├── Synology FICHIERS (stockage documentaire)
- └── Synology ADMINISTRATIFS (données admin/RH)

Système de répartition de charge :

- **Console centrale** qui contrôle le switch
- **3 box** qui font office de **load balancer**
- Basculement automatique selon la charge
- **Destination finale** : serveurs Infomaniak Suisse

Questions pour affiner l'audit :

1. **Les 3 box** : sont-elles identiques ou spécialisées par type de données ?
2. **Console de contrôle** : quel système (Synology DSM, solution tierce) ?
3. **Critères de basculement** : charge CPU, bande passante, disponibilité ?
4. **Monitoring actuel** : logs de basculement disponibles ?

Points d'audit critiques identifiés :

- **SPOF potentiel** : la console centrale de contrôle
- **Cohérence des données** lors des basculements
- **Latence** entre les 3 box et Infomaniak
- **Sécurité** des flux entre catégories (isolation ?)

Méthodologie d'audit sans outils interdits :

- Analyse des logs de basculement
- Test de charge progressive par catégorie
- Vérification des temps de réponse
- Audit des configurations de sécurité

Pouvez-vous détailler le fonctionnement de cette console de contrôle et les critères de basculement ?

Trois box identiques :

3 Synology spécialisés par métier :

- ├── Synology RESSOURCES
- ├── Synology FICHIERS
- └── Synology ADMINISTRATIFS



3 NX identiques (load balancers)



Console centrale (contrôle switch + répartition)



Serveurs Infomaniak Suisse

Architecture précisée :

3 Synology spécialisés par métier :

- ├── Synology RESSOURCES
- ├── Synology FICHIERS
- └── Synology ADMINISTRATIFS



3 NX identiques (load balancers)



Console centrale (contrôle switch + répartition)



Serveurs Infomaniak Suisse

Avantages de cette architecture :

- **Redondance** : 3 NX identiques évitent le SPOF
- **Spécialisation** : chaque Synology dédié à un métier
- **Scalabilité** : répartition de charge dynamique

Points d'audit critiques :

1. Configuration des 3 NX :

- Sont-ils configurés en **active/active** ou **active/passive** ?
- **Algorithme de répartition** : round-robin, least connections, weighted ?
- **Health checks** : monitoring des Synology en amont ?

2. Console centrale :

- **Failover automatique** si un NX tombe ?
- **Logs de basculement** disponibles ?
- **Seuils de basculement** : CPU, mémoire, bande passante ?

3. Sécurité :

- **Isolation** entre les flux des 3 métiers ?
- **Chiffrement** des données vers Infomaniak ?
- **Authentification** entre les couches ?

Méthodologie d'audit adaptée :

- Test de charge par métier (sans outils interdits)
- Analyse des logs de répartition
- Vérification des temps de réponse par NX
- Test de failover (planifié)

3 box. je n'ai pas accès refusé car je fais office de devops junior et non cybersécurité agent ou SOC dans cette configuration et mon stage.

Compris - Limitations d'accès :

En tant que **DevOps junior**, vos accès sont restreints par rapport à un **SOC/CyberSec**. C'est une pratique courante de séparation des rôles.

Audit possible avec vos droits actuels :

Côté utilisateur final :

- **Tests de performance** applicatifs (temps de réponse)
- **Monitoring des applications** déployées
- **Analyse des logs applicatifs** (si accessibles)
- **Tests de charge** depuis le poste utilisateur

Côté infrastructure accessible :

- **Monitoring des services** déployés
- **Métriques système** des applications
- **Analyse des temps de réponse** par métier
- **Documentation** des flux observés

Pour votre mémoire :

- **Partie théorique** : architecture observée et analysée
- **Partie pratique** : déploiement Jitsi et monitoring
- **Recommandations** basées sur l'observation externe

Focus sur la mission Jitsi : C'est là que vous aurez le plus d'autonomie pour :

- Configurer le monitoring
- Tester la montée en charge
- Analyser les performances
- Proposer des optimisations

Question : Avez-vous accès aux serveurs Infomaniak pour déployer Jitsi ou devez-vous passer par l'équipe infrastructure ?

Oui :

Parfait - Accès Infomaniak confirmé :

Vous avez donc autonomie complète sur la partie Jitsi. C'est idéal pour votre mémoire.

Plan d'action pour votre déploiement Jitsi :

Phase 1 : Préparation (1-5 utilisateurs)

- **Installation Jitsi Meet** sur serveur Infomaniak
- **Configuration SSL/TLS** et domaine

- **Monitoring** : CPU, RAM, bande passante
- **Tests** : qualité audio/vidéo, partage d'écran

Phase 2 : Montée en charge (5-15 utilisateurs)

- **Métriques** : latence, perte de paquets
- **Optimisation** : configuration JVB (Jitsi Videobridge)
- **Load balancing** : préparation architecture multi-serveurs

Phase 3 : Scaling (15-50 utilisateurs)

- **Déploiement du load balancer**
- **Sharding** : répartition des conférences
- **Monitoring avancé** : Grafana + Prometheus

Phase 4 : Production (50-500 utilisateurs)

- **Haute disponibilité** : clustering
- **Sécurité** : authentification, chiffrement end-to-end
- **Comparaison avec nujs** (performances, coûts)

Outils de monitoring à prévoir :

- **Jitsi Meet** : statistiques intégrées
- **Serveur** : htop, iostat (autorisés ?)
- **Réseau** : monitoring côté Infomaniak

Question : Quel OS sur les serveurs Infomaniak ? Ubuntu, Debian, CentOS ?

j'ai une ubuntu en ligne sur l'instance infomaniak :Kaas Ubuntu 2404 Kube V1.30

UbuntuExcellent - Configuration technique précisée :

INFRASTRUCTURE JITSU CONFIRMÉE

- **OS** : Ubuntu 24.04 LTS (dernière version stable)
- **Orchestration** : Kubernetes v1.30
- **Plateforme** : Infomaniak KaaS (Kubernetes as a Service)

AVANTAGES DE CETTE STACK

- **Scalabilité native** : K8s gère automatiquement la montée en charge
- **Haute disponibilité** : pods multiples, auto-healing
- **Monitoring intégré** : métriques K8s + possibilité Prometheus/Grafana
- **Load balancing** : Ingress Controller natif

PLAN JITSU REVU POUR KUBERNETES

Phase 1 (1-5 utilisateurs)

- **Déploiement** : Jitsi Meet en pods K8s
- **Services** : ClusterIP pour composants internes

- Ingress : exposition HTTPS avec cert-manager

Phase 2-4 (montée en charge)

- HPA (Horizontal Pod Autoscaler) : scaling automatique
- Resource limits : CPU/RAM par pod
- Monitoring : kubectl top, métriques K8s

OUTILS DISPONIBLES

- kubectl : gestion des pods/services
- helm : déploiement Jitsi (charts disponibles)
- Métriques K8s : monitoring natif sans outils interdits

PROCHAINE SESSION

Préparez les manifests YAML ou Helm charts pour Jitsi sur K8s !

Cette configuration K8s change complètement la donne - vous avez un environnement professionnel moderne pour votre mémoire !

Déjà fait via ma console vscode en mode git-bash, wsl étant une catastrophe et powershell inutile.




Parfait - Setup technique optimal :

CONFIGURATION CONFIRMÉE

- Local : VSCode + Git Bash (choix judicieux)
- Remote : Ubuntu 24.04 + K8s v1.30 sur Infomaniak
- Déploiement : Déjà effectué via kubectl/helm

Git Bash >> PowerShell/WSL pour ce contexte - excellente décision technique.

ÉTAT ACTUEL

-  Jitsi déployé sur K8s
-  Connexion VSCode → Infomaniak
-  Environnement de dev opérationnel

QUESTIONS TECHNIQUES POUR DEMAIN

1. Monitoring : quels outils K8s utilisés ? (kubectl top, dashboard)
2. Performances : résultats des premiers tests 1-5 utilisateurs ?
3. Scaling : HPA configuré ou manuel ?
4. Sécurité : Ingress TLS, network policies ?

FOCUS MÉMOIRE

Avec Jitsi déjà déployé, vous pouvez concentrer votre mémoire sur :

- Analyse comparative : Jitsi vs nujis
- Optimisation : monitoring et scaling K8s
- Sécurité : analyse des flux dans l'architecture globale

- **ROI : coûts Infomaniak vs solution actuelle**
-

Vous avez une excellente base technique pour un mémoire de qualité !

La suite demain avec les documents complémentaires et l'analyse des performances.

RÉCAPITULATIF COMPLET DE VOTRE PROJET

CONTEXTE GÉNÉRAL

- **Formation : Mémoire Licence 3 / Bachelor 3 - Titre RNCP Administrateur Système**
- **Statut : Externe (non stagiaire) avec accès DevOps junior (pas SOC/CyberSec)**
- **Contraintes sécurité : Interdiction Nmap, Netstat, ARP, Lynx**

MISSION 1 : AUDIT TECHNIQUE

Architecture identifiée :

3 Synology spécialisés :

```

├── RESSOURCES
├── FICHIERS
└── ADMINISTRATIFS
  
```

↓

3 box identiques (load balancers)

↓

Console centrale (contrôle switch)

↓

Serveurs Infomaniak Suisse

+ Fibre noire (backup)

Matériel analysé :

- **Machines critiques : APR-F-MEHDI, APR-F-STAGE, KUS-F-UGO (CPU 7e gen, RAM faible)**
- **Vulnérabilités : Spectre/Meltdown, BIOS anciens, stockage mixte**

Limites d'accès :

- **Pas d'accès aux 3 box ni console centrale**
- **Audit possible : côté utilisateur, logs applicatifs, tests de performance**

MISSION 2 : DÉPLOIEMENT JITSI

Objectifs de montée en charge :

- **Phase 1 : 1-5 utilisateurs (installation, config SSL)**
- **Phase 2 : 5-15 utilisateurs (optimisation JVB)**
- **Phase 3 : 15-50 utilisateurs (load balancer)**
- **Phase 4 : 50-500 utilisateurs (clustering, HA)**

Comparaison avec nuji (solution actuelle)

Accès confirmé : Serveurs Infomaniak

PROCHAINES ÉTAPES

- 1. OS des serveurs Infomaniak à identifier**
- 2. Transfert documents supplémentaires**
- 3. Début déploiement Jitsi Phase 1**

Sauvegardez cette synthèse - elle vous servira de base pour reprendre demain !