

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

Noms : LAMBERT-TATHY
Prénoms :Gheorghe-Tony

Document techniques

Contexte du projet – RTL INDUSTRIE

RTL INDUSTRIE est une entreprise spécialisée dans la **vente d'ordinateurs**. Dans le cadre de son expansion, l'entreprise a ouvert un **nouveau site à Lyon (site A)**. Pour soutenir cette implantation stratégique, une **infrastructure réseau complète** a été conçue et déployée, avec pour objectif de répondre aux besoins de **fiabilité, de sécurité, de connectivité intersite** et de **communication client efficace**.

L'architecture repose sur trois zones principales :

- **Le site A** (interne, Lyon)
- **Le site externe** (simulé pour des accès clients/utilisateurs distants)
- **La DMZ** (zone neutre pour l'hébergement du site web et les services accessibles depuis l'extérieur)

L'ensemble de l'infrastructure est interconnecté via des **pare-feu configurés sur pfSense** et un **réseau VPN** simulant les connexions entre les sites.

Dans ce documents je ne parlerais que des réalisations que j'ai réalisées

SOMMAIRE

- 1. Cahier des charges fonctionnel – RTL INDUSTRIE**
- 2. Cahier des charges technique – RTL INDUSTRIE**
- 3. Schéma du réseau RTL INDUSTRIE**
- 4. AP1-Active Directory (HA)**
- 5. AP2- Supervision (Syslog)**
- 6. AP3- Messagerie interne et intersite**
- 7. AP4-Automatisation du service client avec n8n**

Cahier des charges fonctionnel – RTL INDUSTRIE

- Objectif général

Mettre en place une **infrastructure réseau complète et fiable**, destinée à accompagner l'ouverture du site de Lyon de RTL INDUSTRIE, en intégrant les services internes essentiels et un **pôle service client intelligent et automatisé**.

1. Services attendus

Réseau local (LAN)

- Mise en place d'un réseau structuré par **services** (technique, comptabilité, administration).
- Attribution d'**adresses IP fixes** pour les serveurs et équipements critiques.
- Connexion des machines à un **contrôleur de domaine Active Directory**.

Annuaire Active Directory (HA)

- Création de deux **contrôleurs de domaine en haute disponibilité**.
- Gestion des **comptes utilisateurs**, des **groupes**, des **stratégies de sécurité** et des **droits d'accès aux ressources**.
- Intégration de tous les postes clients et serveurs dans le domaine.

Serveur de messagerie

- Installation d'un **serveur de messagerie interne (hMailServer)**.
- Accès des utilisateurs via un **client de messagerie (Thunderbird)**.
- Possibilité d'**envoyer/recevoir des mails entre sites** (y compris depuis l'extérieur).

Site web (DMZ)

- Déploiement d'un **site web professionnel (rtl-industrie.shop)** dans la **DMZ**.
 - Fonctionnalités :
 - Présentation des ordinateurs proposés
 - Formulaire de contact
 - Bouton d'achat simulé (test de processus)
 - Accès sécurisé en **HTTPS** via **reverse proxy**.

Reverse proxy (HA)

- Configuration d'un reverse proxy **en haute disponibilité**.
- Redirection des requêtes vers le webmail, n8n, le site web.
- Gestion centralisée des **certificats SSL/TLS**.

- Protection contre les attaques directes (filtrage, cloisonnement).

Supervision

- Déploiement d'un **serveur Syslog** pour collecter les **logs** du pare-feu et des services critiques.
- Capacité à **tracer les connexions entrantes et sortantes**, détecter les anomalies, produire des alertes.

Automatisation du service client (n8n)

- Mise en place de 3 **workflows automatisés** :

 1. **Réponse automatique aux emails clients** (FAQ, redirection vers assistant IA, ou promesse de réponse humaine).
 2. **Gestion des achats simulés** sur le site :
 - Confirmation envoyée au client
 - Notification au **technicien** (préparation de la commande)
 - Notification au **comptable** (enregistrement de la vente)
 3. **Formulaire de contact** :
 - Réception de la demande
 - Envoi d'un accusé de réception au client
 - Option d'escalade vers l'assistant IA

VPN inter-sites

- Création d'un **VPN site à site** entre :
- Site A (Lyon)
- Site externe (simulation client)

2. Contraintes techniques

- **Adresse IP fixe** pour chaque serveur critique.
- **Nom de domaine interne** : rtl-industrie.local.
- Disponibilité minimale visée : **99 %** (hors coupures de maintenance planifiées).

3. Utilisateurs concernés

Type d'utilisateur	Rôle
Administrateur réseau	Gère les serveurs, les utilisateurs, la supervision
Employé (compta/tech)	Utilise la messagerie, l'accès au wiki, reçoit les commandes
Client externe	Accède au site, contacte l'entreprise, passe commande
Assistant IA	Répond automatiquement aux messages et demandes courantes

Cahier des charges technique – RTL INDUSTRIE

1. Schéma d'adressage IP

Zone	Plage d'adresses	Exemple d'adresses utilisées
Site A	192.168.1.0/24	AD : 192.168.1.200, Mail : 192.168.1.130
Site Externe	192.168.2.0/24	PC Extérieur : 192.168.2.20
DMZ	172.16.1.0/24	Reverse Proxy : 172.16.1.200 / 201, Web : 172.16.1.15

2. Matériel & Machines Virtuelles

Nom du serveur / équipement	IP	Rôle	Système
AD HA 1	192.168.1.200	Contrôleur de domaine principal (Active Directory)	Windows Server
AD HA 2	192.168.1.201	Contrôleur de domaine secondaire	Windows Server
Syslog	192.168.1.160	Serveur de supervision (Syslog + Nagios)	Debian
Serveur Wiki (VM 1 & 2)	192.168.1.101/102	Documentation technique interne (wiki)	Debian / Wiki.js
Serveur Mail + n8n	192.168.1.130	Messagerie locale + automatisation via n8n	Windows Server
PC Compta / PC Tech	192.168.1.140/141	Utilisateurs internes	Windows 10
Pare-feu Site A (interne)	192.168.1.230	Contrôle et filtrage du réseau interne / VPN vers DMZ & externe	pfSense

Pare-feu Site externe	192.168.2.230	Contrôle des flux client externe / VPN vers DMZ & site A	pfSense
Pare-feu DMZ	172.16.1.230	Protection de la zone DMZ, NAT et redirection HTTPS vers serveur web	pfSense
Reverse Proxy	172.16.1.200	Gère exclusivement l'accès HTTPS au serveur web	Debian + NGINX
Serveur Web (site vitrine)	172.16.1.15	Site rtlindustrie.shop, formulaire de contact et page produits	Debian + Apache
PC Extérieur / Test	192.168.2.10/20	Simulation d'accès client depuis l'extérieur	Windows

3. Logiciels & Services installés

Sécurité / Réseau

- **pfSense** : pare-feu (x3)
- **VPN IPsec** : tunnel sécurisé inter-sites
- **Reverse Proxy (NGINX/HAProxy)** : gestion des accès et certificats TLS

Annuaire

- **Active Directory (Windows Server)** en HA
- **GPO** pour sécurisation des postes, mappage réseau, etc.

Communication

- **hMailServer** pour la messagerie
- **Thunderbird** pour client de messagerie

Automatisation

- **n8n** (sur serveur mail) :
- 3 workflows automatisés (email, achat, contact)
- Liaison à l'assistant IA via webhook/API
- Notification par email aux services concernés

Documentation

- **Wiki.js** ou équivalent sur serveur VM 101/102

Supervision

- **Syslog-ng ou rsyslog**
 - Centralisation des journaux des pare-feux et des services critiques
 - Journalisation quotidienne, alerte sur activité anormale
-

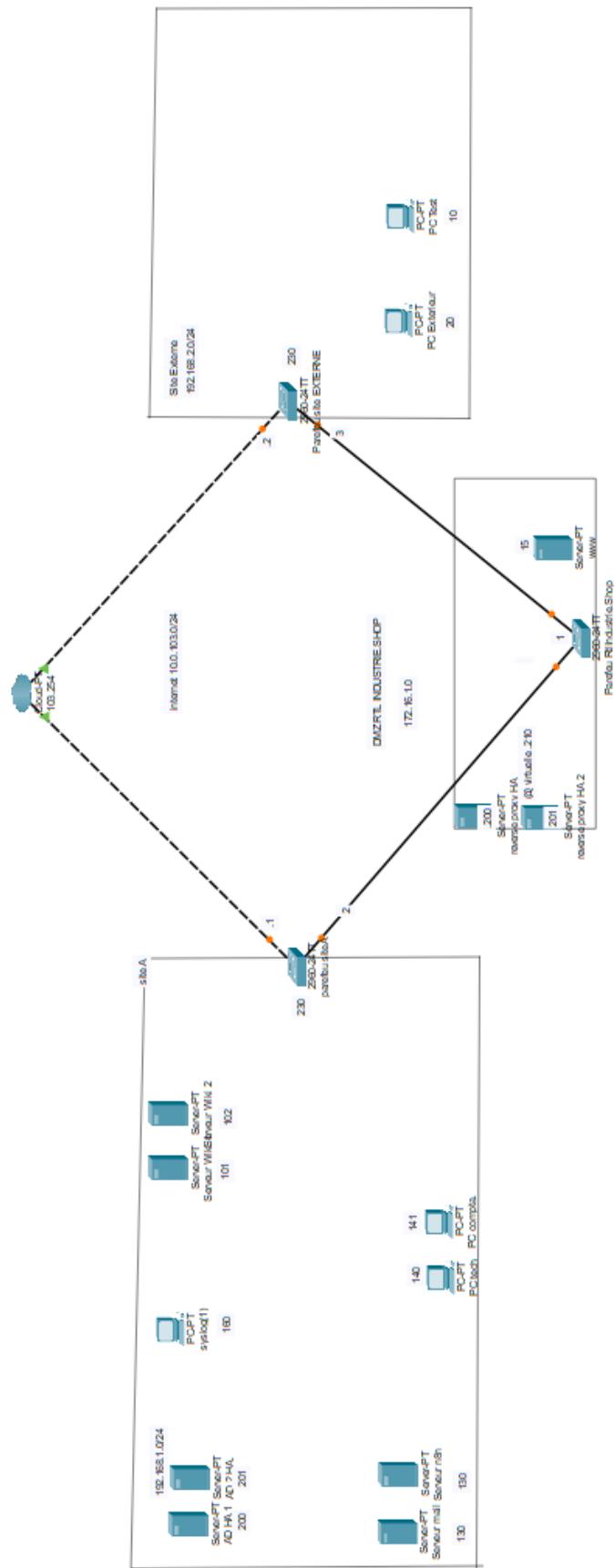
4. Services exposés (via reverse proxy)

Service	URL	Port(s)	Sécurisé
Site Web	https:// rtlindustrie.shop	443	HTTPS

5. Performances et redondance

- **Haute disponibilité** sur les contrôleurs de domaine et le reverse proxy
- **Surveillance continue** via Syslog
- **Redondance réseau** via VPN entre sites

Schéma du réseau RTL INDUSTRIE



AP1- Active Directory (HA)

Dans le cadre du déploiement de son infrastructure informatique au sein du **site A (Lyon)**, RTL INDUSTRIE a souhaité mettre en place une **authentification centralisée et résiliente** pour la gestion des utilisateurs, des groupes et des politiques de sécurité.

La solution choisie repose sur **deux contrôleurs de domaine Windows Server en haute disponibilité**, afin d'assurer la **continuité d'accès et la réplication des services d'annuaire**.

Le service Active Directory permet de :

- Centraliser la **gestion des identités utilisateurs et groupes**
- Appliquer des **stratégies de sécurité (GPO)**
- Authentifier les accès à la messagerie, au réseau et aux ressources partagées
- Maintenir une **tolérance aux pannes (site local)**

Objectifs techniques du projet

- Déployer **2 contrôleurs de domaine AD** en haute disponibilité.
- Intégrer tous les serveurs et postes clients au domaine.
- Implémenter des **GPO ciblées** pour chaque groupe d'utilisateurs.
- Permettre une **authentification fiable** des services internes (messagerie, n8n).
- Surveiller le bon fonctionnement du domaine.

Architecture retenue

Composant	Description
Contrôleur principal	Windows Server 2025 – IP : 192.168.1.200
Contrôleur secondaire	Windows Server 2025 – IP : 192.168.1.201
Domaine	rtl-industrie.local
DNS intégré	AD DNS
Postes clients	Intégrés au domaine, authentification via AD
Services dépendants	Serveur mail, n8n, Thunderbird, supervision

Mise en œuvre détaillée

Installation des contrôleurs de domaine

1. **Déploiement de 2 VM Windows Server 2025**
2. Installation du rôle Active Directory Domain Services + DNS
3. Création d'une nouvelle forêt sur le serveur 1 :

Domaine : rtl-industrie.local

4. Ajout du second serveur comme **contrôleur secondaire** du même domaine
5. **Test de réplication :**
 - repadmin /replsummary
 - dcdiag

Création des objets du domaine

OU créées :

- Utilisateurs
- Groupes
- Postes

Utilisateurs ajoutés :

- Ralph – membre du groupe comptta
- Lucas – membre du groupe tech

Groupes créés :

- comptta, tech

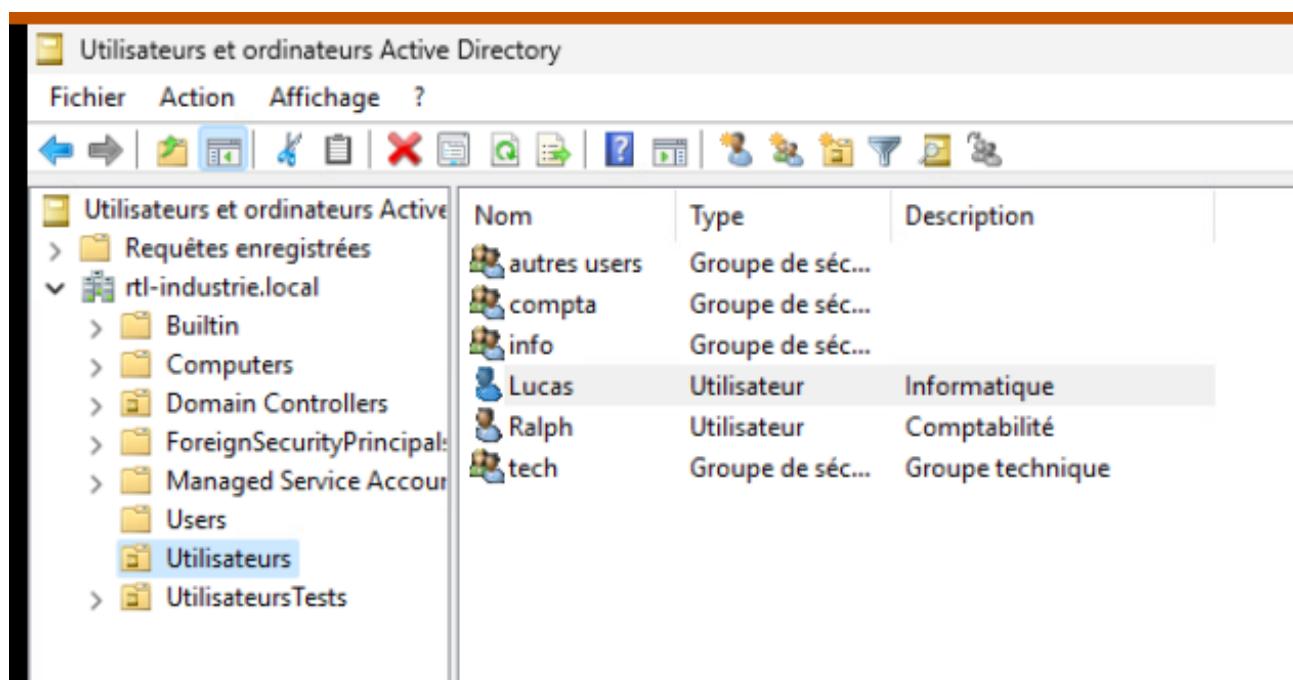
Production livrée

- Domaine rtl-industrie.local fonctionnel
- Authentification validée depuis tous les postes clients
- Réplication AD fonctionnelle
- 2 utilisateurs créés, affectés aux bons groupes
- GPO déployées avec succès

- Les autres services (mail, n8n) intègrent l'authentification AD
-

Conclusion

Le service Active Directory assure à RTL INDUSTRIE une **structure d'authentification centralisée**, garantissant à la fois **performance et haute disponibilité**. Il constitue le **socle principal de l'architecture réseau** et permet à tous les services et utilisateurs de fonctionner de manière cohérente et sécurisée.



The screenshot shows the Windows Active Directory Users and Computers management console. The left pane displays the organizational structure of the domain 'rtl-industrie.local'. The 'Utilisateurs' folder is selected. The right pane is a table listing objects in the selected folder:

Nom	Type	Description
autres users	Groupe de séc...	
compta	Groupe de séc...	
info	Groupe de séc...	
Lucas	Utilisateur	Informatique
Ralph	Utilisateur	Comptabilité
tech	Groupe de séc...	Groupe technique

Sur cette image nous pouvons apercevoir le nom de domaine qui est rtl-industrie.local, les différents groupes créés qui sont: Compta et tech et les différents utilisateurs créés : Ralph (qui est le comptable) et Lucas (qui est le technicien).

AP2- Supervision (Syslog)

Dans le cadre du renforcement de la sécurité réseau et de la traçabilité des événements critiques, RTL INDUSTRIE a souhaité mettre en place une solution de supervision **légère et ciblée**, centrée sur la **collecte des journaux du pare-feu du site A**.

L'objectif est de disposer d'un **point central de collecte** des logs pour le pare-feu (pfSense – 192.168.1.230), afin de détecter les anomalies réseau, surveiller les règles de filtrage, et conserver un historique des événements réseau.

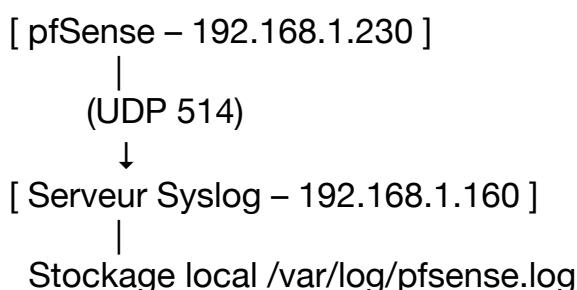
Objectifs techniques du projet

- Installer un **serveur Syslog** sous Debian sur le réseau interne.
 - Configurer le pare-feu pfSense pour qu'il envoie ses logs vers le serveur Syslog.
 - Filtrer, trier et archiver localement les logs reçus.
 - Intégrer cette supervision dans la stratégie de **veille réseau**.
-

Architecture retenue

Composant	Description
Serveur Syslog	Debian 12 – IP : 192.168.1.160
Collecteur logs	rsyslog, écoute sur port UDP 514
Source surveillée	Pare-feu pfSense (site A) – 192.168.1.230

Schéma simplifié du service



Mise en œuvre détaillée

1. Installation du serveur Syslog

- Déploiement d'une machine virtuelle sous Debian 12.
- Installation de rsyslog :

```
sudo apt update
sudo apt install rsyslog
```

2. Configuration du port d'écoute

- Fichier /etc/rsyslog.conf :

```
module(load="imudp")
input(type="imudp" port="514")
```

- Redémarrage du service :

```
sudo systemctl restart rsyslog
```

3. Configuration de pfSense

- Interface Web > Status > System Logs > Settings
- Section “Remote Logging Options” :
- **Enable Remote Logging** : activé
- **Target IP** : 192.168.1.160
- **Port** : 514
- **Facility** : sélection de tout

Comme montrer sur l'image si dessous

Remote Logging Options

Enable Remote Logging Send log messages to remote syslog server

Source Address: LAN

This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If a single IP is picked, remote syslog servers must all be of that IP type. To mix IPv4 and IPv6 remote syslog servers, bind to all interfaces.

NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.

IP Protocol: IPv4

This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; if an IP address of the selected type is not found on the chosen interface, the other type will be tried.

Remote log servers: 192.168.1.160:514

Remote Syslog Contents: Everything, System Events, Firewall Events, DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns), DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client), PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client), General Authentication Events, Captive Portal Events, VPN Events (IPsec, OpenVPN, L2TP, PPPoE Server), Gateway Monitor Events, Routing Daemon Events (RADVD, UPnP, RIP, OSPF, BGP), Network Time Protocol Events (NTP Daemon, NTP Client), Wireless Events (hostapd)

Activer Windows
Accédez aux paramètres pour activer Windows.

Journalisation et filtrage

- Les logs sont redirigés vers un fichier personnalisé :
- Exemple dans /etc/rsyslog.d/pfsense.conf :

```
if ($fromhost-ip == '192.168.1.230') then /var/log/pfsense.log & stop
```

```

Jun 7 23:59:28 192.168.1.230 charon[2082]: 13[IKE] <con1142828> activating IKE_DPD task
Jun 7 23:59:28 192.168.1.230 charon[2082]: 13[ENC] <con1142828> generating INFORMATIONAL request 493 []
Jun 7 23:59:28 192.168.1.230 charon[2082]: 13[NET] <con1142828> sending packet: from 10.0.103.1[500] to 10.0.103.2[500] (57 bytes)
Jun 7 23:59:28 192.168.1.230 charon[2082]: 13[NET] <con1142828> received packet: from 10.0.103.2[500] to 10.0.103.1[500] (57 bytes)
Jun 7 23:59:28 192.168.1.230 charon[2082]: 13[ENC] <con1142828> parsed INFORMATIONAL response 493 []
Jun 7 23:59:28 192.168.1.230 charon[2082]: 13[IKE] <con1142828> activating new tasks
Jun 7 23:59:28 192.168.1.230 charon[2082]: 13[IKE] <con1142828> nothing to initiate
Jun 7 23:59:38 192.168.1.230 charon[2082]: 13[IKE] <con1142828> sending DPD request
Jun 7 23:59:38 192.168.1.230 charon[2082]: 13[IKE] <con1142828> queueing IKE_DPD task
Jun 7 23:59:38 192.168.1.230 charon[2082]: 13[IKE] <con1142828> activating new tasks
Jun 7 23:59:38 192.168.1.230 charon[2082]: 13[IKE] <con1142828> activating IKE_DPD task
Jun 7 23:59:38 192.168.1.230 charon[2082]: 13[ENC] <con1142828> generating INFORMATIONAL request 494 []
Jun 7 23:59:38 192.168.1.230 charon[2082]: 13[NET] <con1142828> sending packet: from 10.0.103.1[500] to 10.0.103.2[500] (57 bytes)
Jun 7 23:59:38 192.168.1.230 charon[2082]: 13[NET] <con1142828> received packet: from 10.0.103.2[500] to 10.0.103.1[500] (57 bytes)
Jun 7 23:59:38 192.168.1.230 charon[2082]: 13[ENC] <con1142828> parsed INFORMATIONAL response 494 []
Jun 7 23:59:38 192.168.1.230 charon[2082]: 13[IKE] <con1142828> activating new tasks
Jun 7 23:59:38 192.168.1.230 charon[2082]: 13[IKE] <con1142828> nothing to initiate
Jun 7 23:59:48 192.168.1.230 charon[2082]: 13[IKE] <con1142828> sending DPD request
Jun 7 23:59:48 192.168.1.230 charon[2082]: 13[IKE] <con1142828> queueing IKE_DPD task
Jun 7 23:59:48 192.168.1.230 charon[2082]: 13[IKE] <con1142828> activating new tasks
Jun 7 23:59:48 192.168.1.230 charon[2082]: 13[IKE] <con1142828> activating IKE_DPD task
Jun 7 23:59:48 192.168.1.230 charon[2082]: 13[ENC] <con1142828> generating INFORMATIONAL request 495 []
Jun 7 23:59:48 192.168.1.230 charon[2082]: 13[NET] <con1142828> sending packet: from 10.0.103.1[500] to 10.0.103.2[500] (57 bytes)
Jun 7 23:59:48 192.168.1.230 charon[2082]: 13[NET] <con1142828> received packet: from 10.0.103.2[500] to 10.0.103.1[500] (57 bytes)
Jun 7 23:59:48 192.168.1.230 charon[2082]: 13[ENC] <con1142828> parsed INFORMATIONAL response 495 []
Jun 7 23:59:48 192.168.1.230 charon[2082]: 13[IKE] <con1142828> activating new tasks
Jun 7 23:59:48 192.168.1.230 charon[2082]: 13[IKE] <con1142828> nothing to initiate
Jun 7 23:59:56 localhost systemd[1]: session-9708.scope: Deactivated successfully.
Jun 7 23:59:56 localhost systemd[1]: session-9706.scope: Deactivated successfully.
Jun 8 00:00:01 192.168.1.230 charon[2082]: 13[IKE] <con1142828> sending DPD request
Jun 8 00:00:01 192.168.1.230 charon[2082]: 13[IKE] <con1142828> queueing IKE_DPD task
Jun 8 00:00:01 192.168.1.230 charon[2082]: 13[IKE] <con1142828> activating new tasks
Jun 8 00:00:01 192.168.1.230 charon[2082]: 13[ENC] <con1142828> generating INFORMATIONAL request 496 []
Jun 8 00:00:01 192.168.1.230 charon[2082]: 13[NET] <con1142828> sending packet: from 10.0.103.1[500] to 10.0.103.2[500] (57 bytes)
Jun 8 00:00:01 192.168.1.230 charon[2082]: 13[NET] <con1142828> received packet: from 10.0.103.2[500] to 10.0.103.1[500] (57 bytes)
Jun 8 00:00:01 192.168.1.230 charon[2082]: 13[ENC] <con1142828> parsed INFORMATIONAL response 496 []
Jun 8 00:00:01 192.168.1.230 charon[2082]: 13[IKE] <con1142828> activating new tasks
Jun 8 00:00:01 192.168.1.230 charon[2082]: 13[IKE] <con1142828> nothing to initiate
Jun 8 00:00:01 localhost systemd[1]: Starting system activity accounting tool...
Jun 8 00:00:01 localhost systemd[1]: Starting Rotate log files...
Jun 8 00:00:01 localhost systemd[1]: sysstat-collect.service: Deactivated successfully.
Jun 8 00:00:01 localhost systemd[1]: Finished system activity accounting tool.
Jun 8 00:00:01 localhost systemd[1]: Started Session 9709 of User apache.
Jun 8 00:00:01 localhost systemd[1]: Started Session 9711 of User nagios.
Jun 8 00:00:01 localhost systemd[1]: Started Session 9718 of User nagios.
Jun 8 00:00:01 localhost systemd[1]: Started Session 9712 of User nagios.
Jun 8 00:00:01 localhost systemd[1]: Reloading The Apache HTTP Server...
Jun 8 00:00:01 localhost systemd[1]: session-9711.scope: Deactivated successfully.

```

Production livrée

- Le pare-feu pfSense envoie correctement ses logs réseau.
 - Le serveur Syslog reçoit, filtre et archive les événements dans /var/log/pfsense.log.
 - Les journaux sont disponibles pour **audit, analyse et incident response**.
-

Conclusion

La solution de supervision Syslog installée chez RTL INDUSTRIE répond aux besoins de **surveillance ciblée** et de **centralisation des journaux du pare-feu du site A**. Elle constitue une base solide pour une politique de sécurité réseau, tout en restant légère, simple à maintenir et évolutive.

AP-3 Messagerie interne et intersite

1. Contexte du projet

Dans le cadre de la mise en place de son infrastructure informatique, RTL INDUSTRIE a souhaité déployer un système de **messagerie interne complet**, capable de gérer les communications entre les collaborateurs sur le site principal (site A), mais également de permettre des **échanges simulés avec des utilisateurs externes**, comme s'ils étaient des clients situés hors réseau.

Ce double objectif a été réalisé via l'installation de **deux serveurs hMailServer** configurés sur des plages réseau distinctes : l'un pour le **réseau interne**, et l'autre pour un **réseau externe simulé**.

2. Objectifs techniques

- Déployer un serveur de messagerie interne accessible aux collaborateurs.
 - Simuler un environnement client externe avec un second serveur de messagerie.
 - Assurer l'échange complet de mails entre les deux environnements.
 - Créer des comptes dédiés par rôle pour faciliter l'organisation des échanges.
 - Fournir une interface simple via Thunderbird.
-

3. Architecture retenue

Composant	Description
Serveur mail interne	hMailServer – IP : 192.168.1.130 – domaine mail.rtl-industrie.local
Serveur mail externe simulé	hMailServer – IP : 192.168.2.20 – domaine mail.exterieur.com
Clients internes	Thunderbird (installé sur les postes du site A)
Client externe simulé	Thunderbird sur PC distant (site extérieur)

4. Schéma simplifié

[Client Externe – Thunderbird]

(192.168.2.20)



[hMailServer – 192.168.2.20]

(mail.exterieur.com)

↑↓ SMTP/IMAP

[hMailServer – 192.168.1.130]

(mail.rtl-industrie.local)



[Postes internes – Thunderbird]

5. Mise en œuvre détaillée

5.1 Installation des serveurs

- Deux machines Windows Server ont été déployées avec hMailServer :
- **Serveur A (interne)** → IP : 192.168.1.130 – mail.rtl-industrie.local
- **Serveur B (externe simulé)** → IP : 192.168.2.20 – mail.exterieur.com
- Ports SMTP (25) et IMAP (143) ouverts sur chaque serveur
- Les DNS internes ont été configurés pour la résolution des domaines respectifs

5.2 Comptes créés sur le serveur interne

Adresse mail Utilisation

ralph@mail.rtl-industrie.local

Utilisateur comptable

lucas@mail.rtl-industrie.local

Utilisateur technicien

contact@mail.rtl-industrie.local

Adresse de contact général de l'entreprise

faq@mail.rtl-industrie.local

Adresse dédiée aux questions fréquentes

support@mail.rtl-industrie.local

Adresse pour les échanges liés aux commandes

Name	Enabled
contact@mail.rtl-industrie.local	Yes
faq@mail.rtl-industrie.local	Yes
lucas@mail.rtl-industrie.local	Yes
ralph@mail.rtl-industrie.local	Yes
support@mail.rtl-industrie.local	Yes

5.3 Compte simulé sur le serveur externe

Adresse mail Utilisation simulée

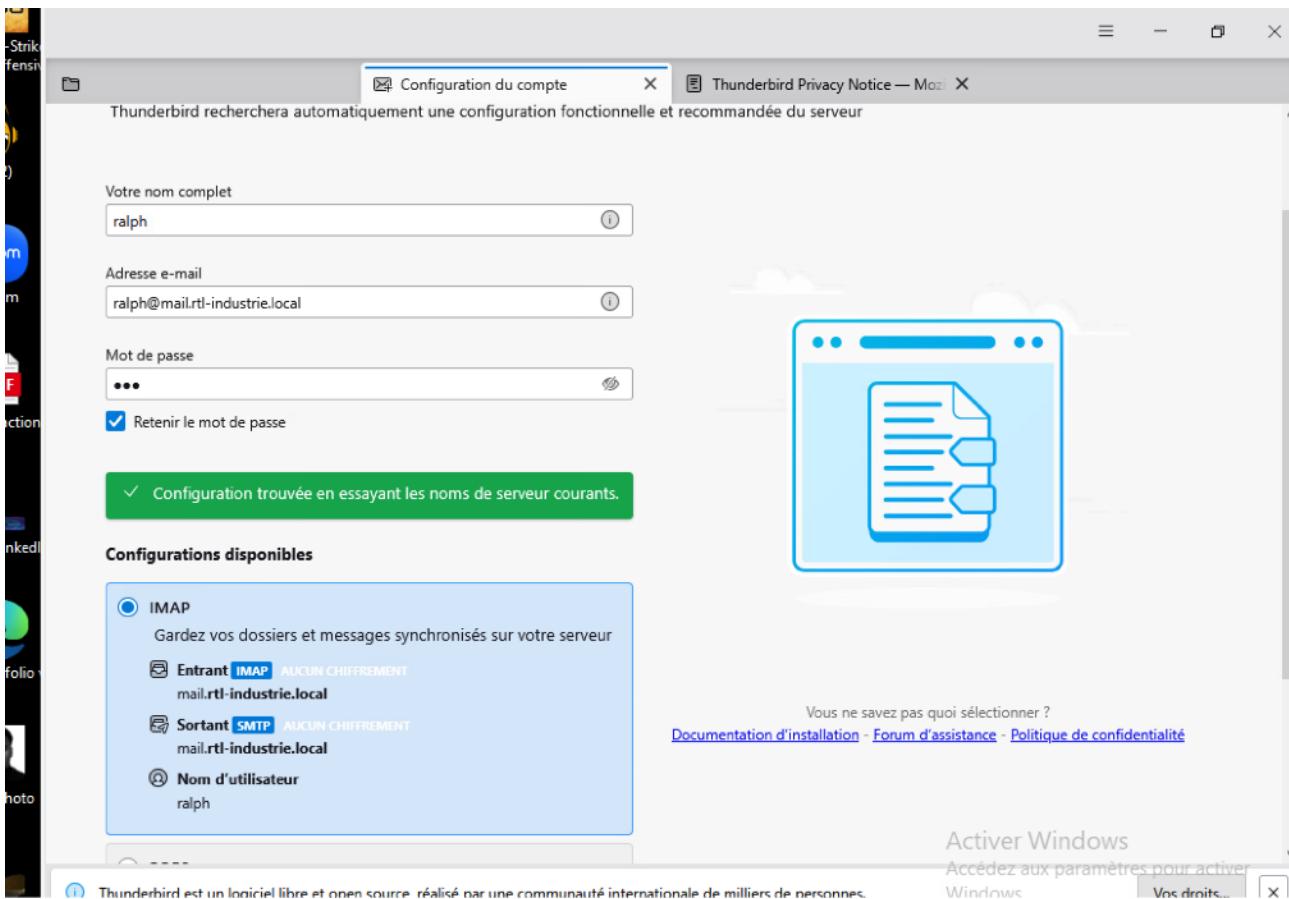
client@mail.exterieur.com Simulation d'un client réel

Name	Enabled
client@mail.exterieur.com	Yes

5.4 Configuration des clients Thunderbird

• Postes internes (site A) :

- Serveur entrant (IMAP) : 192.168.1.130 – port 143
- Serveur sortant (SMTP) : 192.168.1.20 – port 25
- Comptes Ralph et Lucas configurés comme nous pouvons le voir sur l'image.

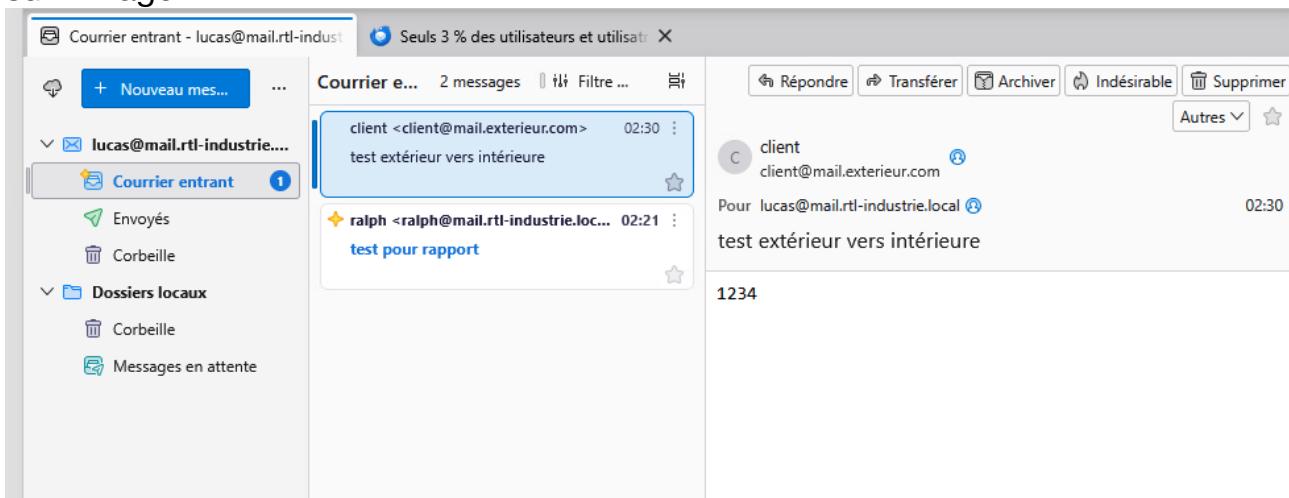


• Poste externe simulé (site externe) :

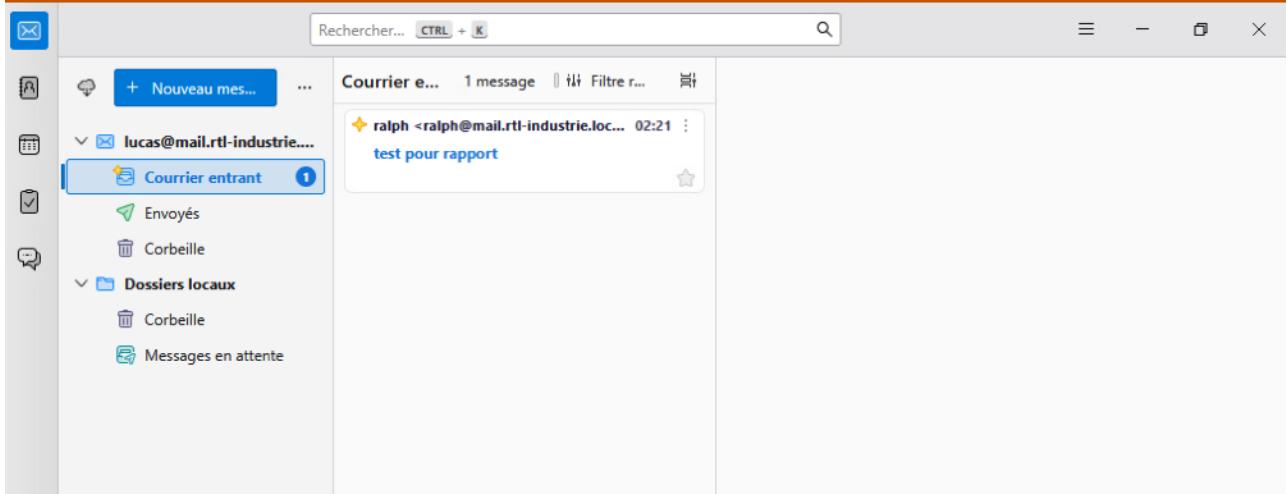
- Serveur entrant (IMAP) : 192.168.2.20 – port 143
- Serveur sortant (SMTP) : 192.168.2.20 – port 25
- Compte client@mail.exterieur.com configuré

6. Résultats et vérifications

- Un mail envoyé depuis client@mail.exterieur.com vers lucas@mail.rtl-industrie.local est bien **reçu par le serveur interne**. comme nous pouvons le voir sur l'image.



- Les utilisateurs Ralph et Lucas peuvent échanger des mails sans problème via le serveur 192.168.1.130. comme nous pouvons le voir sur l'image.



- La résolution des noms de domaine fonctionne dans chaque environnement (grâce aux DNS locaux).
-

8. Conclusion

Cette infrastructure de messagerie à deux serveurs offre à RTL INDUSTRIE une **plateforme fonctionnelle et réaliste** pour simuler tous les scénarios de communication, aussi bien internes qu'externes. Elle permet de tester les processus de contact, de réception et de réponse dans des conditions proches de la production réelle.

AP4-Automatisation du service client avec n8n

1. Contexte du projet

Afin de moderniser son pôle service client, RTL INDUSTRIE a mis en place une plateforme d'automatisation à l'aide de **n8n**, hébergée sur un serveur interne. Cette solution permet de :

- Répondre automatiquement aux emails des clients.
 - Traiter les formulaires de contact reçus depuis le site web.
 - Gérer les commandes simulées via un bouton “Acheter” sur les fiches produit.
 - Soulager les équipes techniques et comptables en automatisant la notification interne.
-

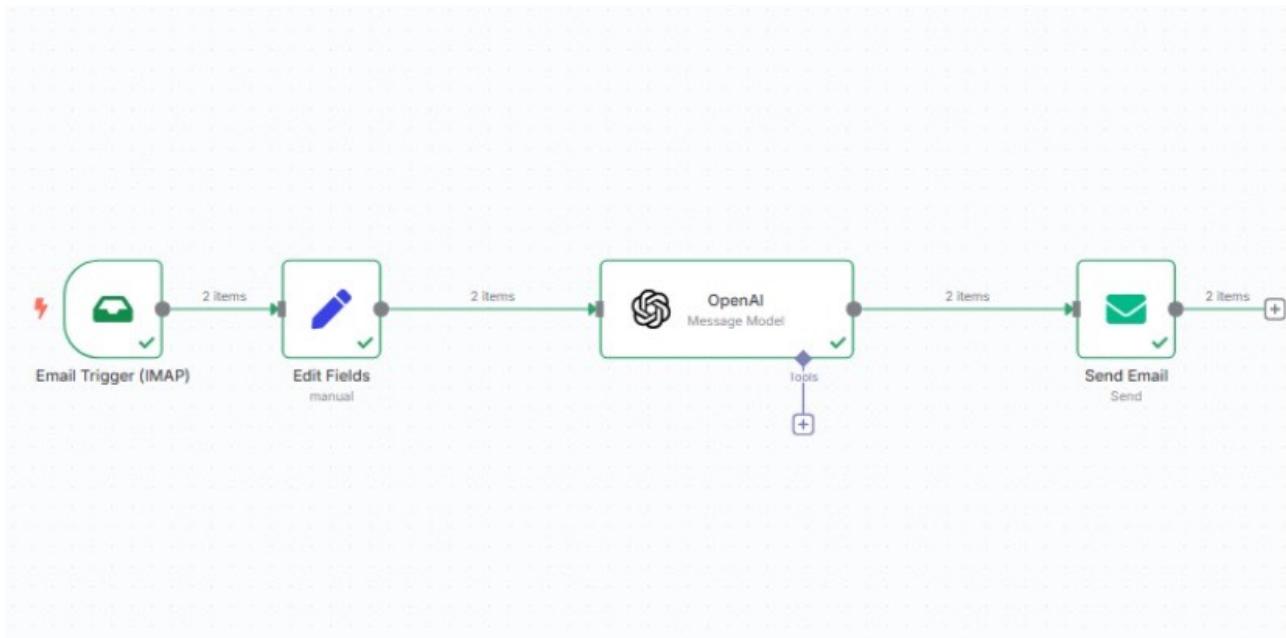
2. Objectifs techniques

- Installer n8n sur le serveur 192.168.1.130.
- Sécuriser l'accès à n8n via un reverse proxy HTTPS (<https://n8n.rtl-industrie.local:5678>).
- Mettre en œuvre trois workflows principaux :
- Traitement automatique des emails entrants.
- Traitement d'une commande en ligne.
- Traitement du formulaire de contact.
- Intégrer un assistant IA basé sur OpenRouter GPT-4.
- Connecter le tout avec les serveurs de messagerie internes (IMAP/SMTP).

3. Architecture retenue

Composant	Détails techniques
Serveur n8n	Windows Server – IP : 192.168.1.130
Adresse d'accès	https://n8n.rtl-industrie.local:5678 (via reverse proxy)
IA intégrée	OpenRouter GPT-4 (API Key sécurisée dans Credentials)
Emails surveillés	faq@mail.rtl-industrie.local, contact@..., support@...
Déclencheurs	Webhooks HTTP (site) + IMAP (mails entrants)

4. Workflow 1 – Réponse automatique aux emails (FAQ)



Déclencheur :

- **IMAP Email** : Surveille l'adresse faq@mail.rtl-industrie.local.
- Paramètres :
- Host : 192.168.1.230
- Port : 143
- Secure : false
- User : faq@mail.rtl-industrie.local
- Password : RTLINDUSTRIE69@

Nœud IA :

- **OpenRouter (GPT-4)** avec le prompt suivant :

Tu es un assistant IA pour l'entreprise RTL INDUSTRIE. Ta tâche est de répondre de manière professionnelle, polie et concise aux questions fréquentes des clients concernant :

- La gamme de PC vendus (PRO-01, BURO-02, CONFORT-03, GAMER-04, GAMÉR-05)
- Les délais de livraison
- Les moyens de paiement
- Le support client

Si tu ne connais pas la réponse, dis simplement : "Votre message a bien été pris en compte, notre équipe vous répondra rapidement."

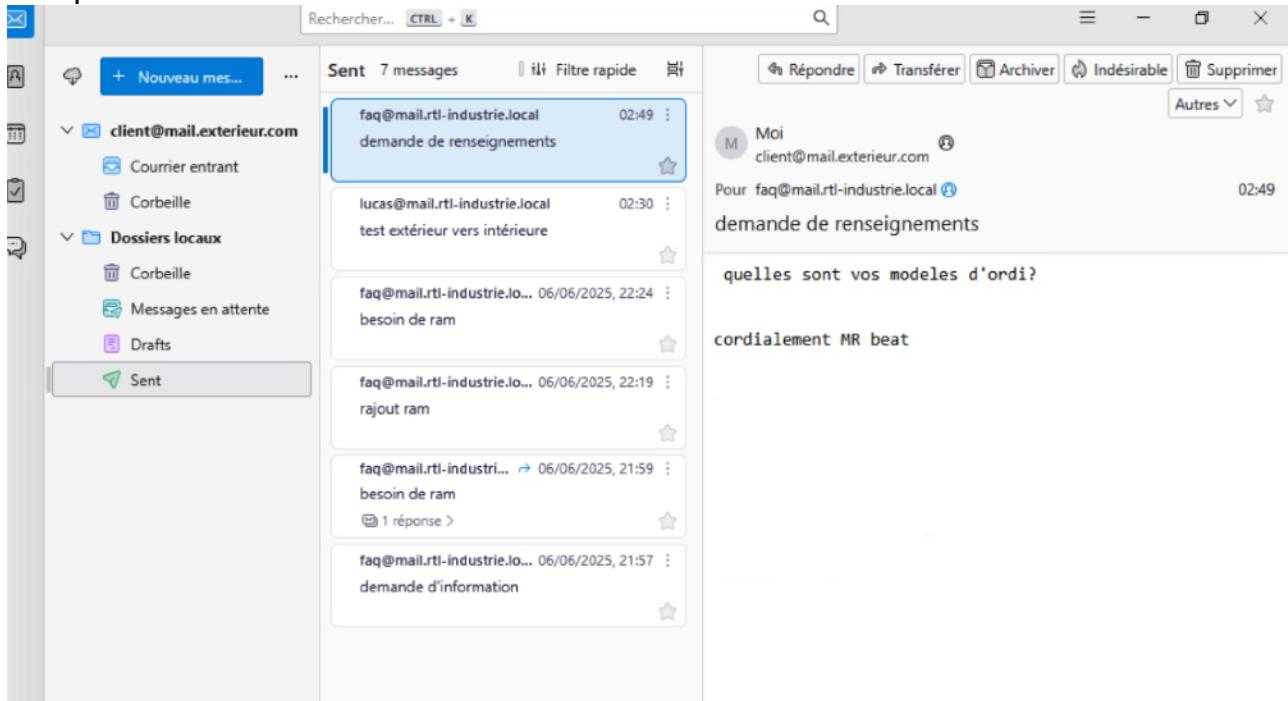
Signature à ajouter à la fin :

Cordialement,
L'équipe RTL INDUSTRIE
✉ faq@mail.rtl-industrie.local
🌐 rtlindustrie.shop

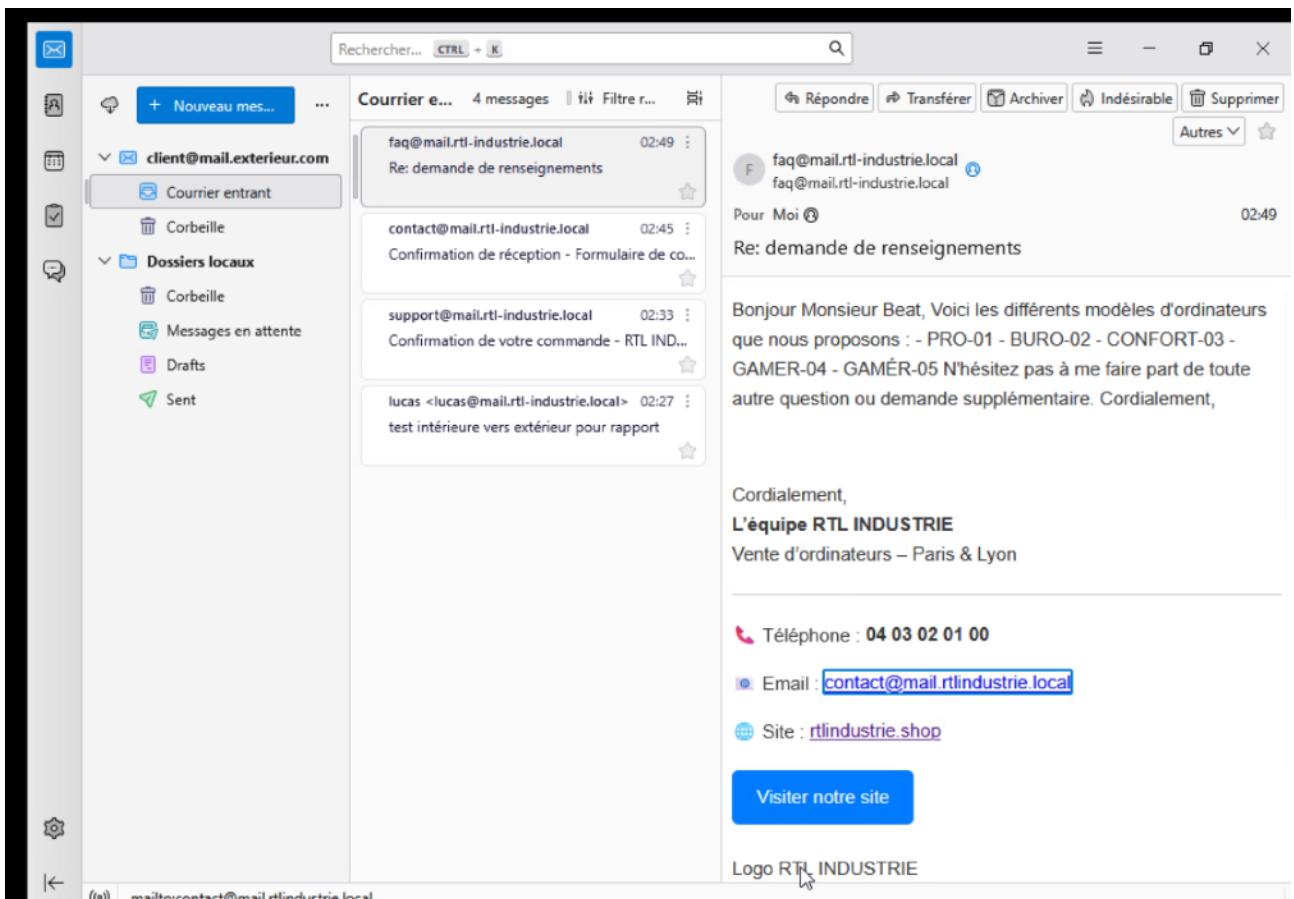
Nœud Send Email :

- Envoie la réponse générée au client.

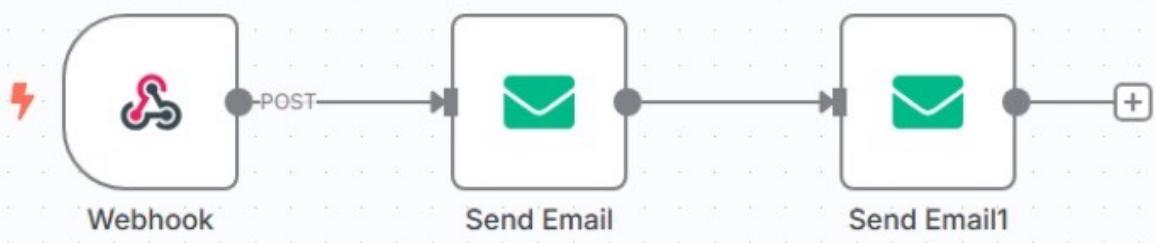
Ce que le client envoie:



Ce qu'il reçoit:



5. Workflow 2 – Formulaire de contact



Déclencheur :

- **Webhook HTTP :**
- URL : <https://n8n.rtl-industrie.local:5678/webhook/contact>
- Méthode : POST
- Authentification : aucune (réservé à réseau interne)

Liaison HTML sur le site (extrait code) :

```
<form action="https://n8n.rtl-industrie.local:5678/webhook/contact" method="POST">
  <input type="text" name="nom" placeholder="Votre nom">
  <input type="email" name="email" placeholder="Votre adresse email">
  <textarea name="message" placeholder="Votre message"></textarea>
  <button type="submit">Envoyer</button>
</form>
```

Nœud Send Email :

- Envoie automatiquement un mail d'accusé de réception :

Objet : Accusé de réception – RTL INDUSTRIE

Bonjour {{nom}},

Nous avons bien reçu votre message :
“{{message}}”

Notre équipe vous répondra dans les plus brefs délais.
Pour toute question fréquente, contactez faq@mail.rtl-industrie.local.

Cordialement,
L'équipe RTL INDUSTRIE

 contact@mail.rtl-industrie.local

 rtlindustrie.shop

Nœud Send Email 1:

- Envoi le mail au contact@mail.rtl-industrie.local

Le client remplis ce formulaire sur le site :

RTL INDUSTRIE - Ordinateurs Non sécurisé <https://rtl-industrie.shop>

Nous contacter

Nom
Daniel

Email
client@mail.exterieur.com

Message
test pour rapport

Envoyer

© 2025 RTL INDUSTRIE — Tous droits réservés · [rtlindustrie.shop](https://rtl-industrie.shop) · Contact : 04 03 02 01 00 · contact@mail.rtl-industrie.local

Et reçoit un accusé de réception :

Courrier e... 3 messages

client@mail.exterieur.com

Courrier entrant

Corbeille

Dossiers locaux

Corbeille

Messages en attente

Drafts

Sent

contact@mail.rtl-industrie.local 02:45 : Confirmation de réception - Formulaire de co...

support@mail.rtl-industrie.local 02:33 : Confirmation de votre commande - RTL IND...

lucas <lucas@mail.rtl-industrie.local> 02:27 : test intérieure vers extérieur pour rapport

Répondre **Transférer** **Archiver** **Indésirable** **Supprimer** **Autres**

contact@mail.rtl-industrie.local 02:45
Pour Moi Confirmation de réception - Formulaire de contact

Bonjour Daniel,

Nous avons bien reçu votre message :
test pour rapport

Notre équipe vous répondra dans les meilleurs délais.
Pour toute autre demande, n'hésitez pas à contacter notre assistant IA par mail à faq@mail.rtl-industrie.local.

Merci pour votre confiance.
L'équipe RTL INDUSTRIE

Téléphone : 04 03 02 01 00

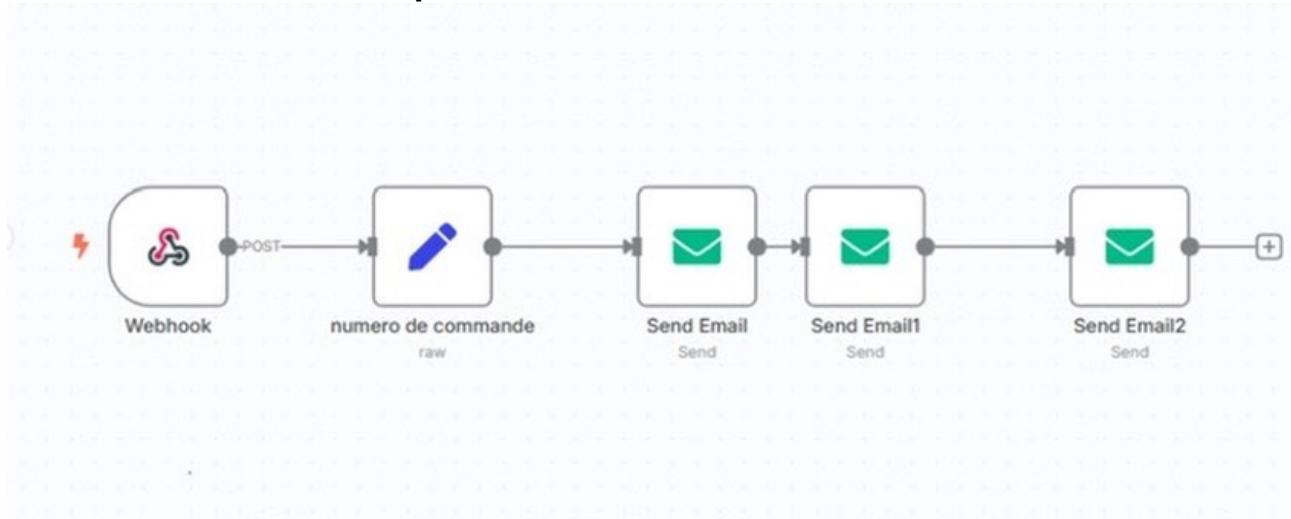
Email : contact@mail.rtl-industrie.local

Site : rtl-industrie.shop

Visiter notre site

mailto:contact@mail.rtlindustrie.local

6. Workflow 3 – Achat depuis le site web



Déclencheur :

- **Webhook HTTP**
- URL : <https://n8n.rtl-industrie.local/webhook/achat>
- Déclenché par le bouton “Acheter” dans le code HTML :

```
<form action="https://n8n.rtl-industrie.local:5678/webhook/achat"
method="POST">
  <input type="hidden" name="produit" value="PRO-01">
  <input type="text" name="nom" placeholder="Nom complet">
  <input type="email" name="email" placeholder="Email">
  <button type="submit">Acheter</button>
</form>
```

Nœuds numéros de commande : pour créer un numéro de commande unique

Nœuds internes :

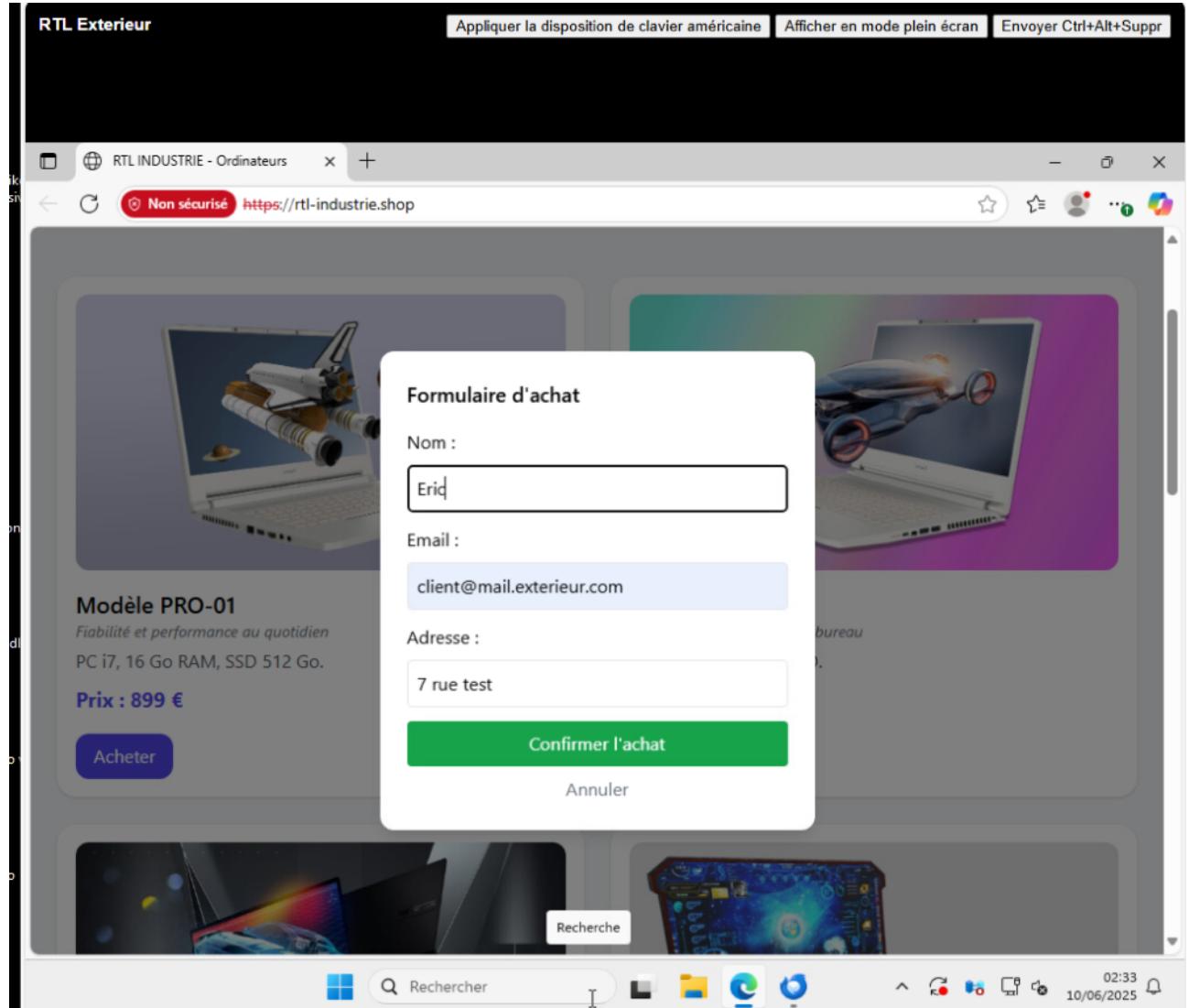
- **Send Email (Client)** :
 - Objet : Confirmation de commande
 - Contenu HTML : Détail de l'achat + lien vers rtlindustrie.shop
- **Send Email (Technicien)** :
 - Adresse : lucas@mail.rtl-industrie.local
 - Contenu :

Nouvelle commande : {{produit}}
Client : {{nom}}, {{email}}
Merci de préparer la commande.

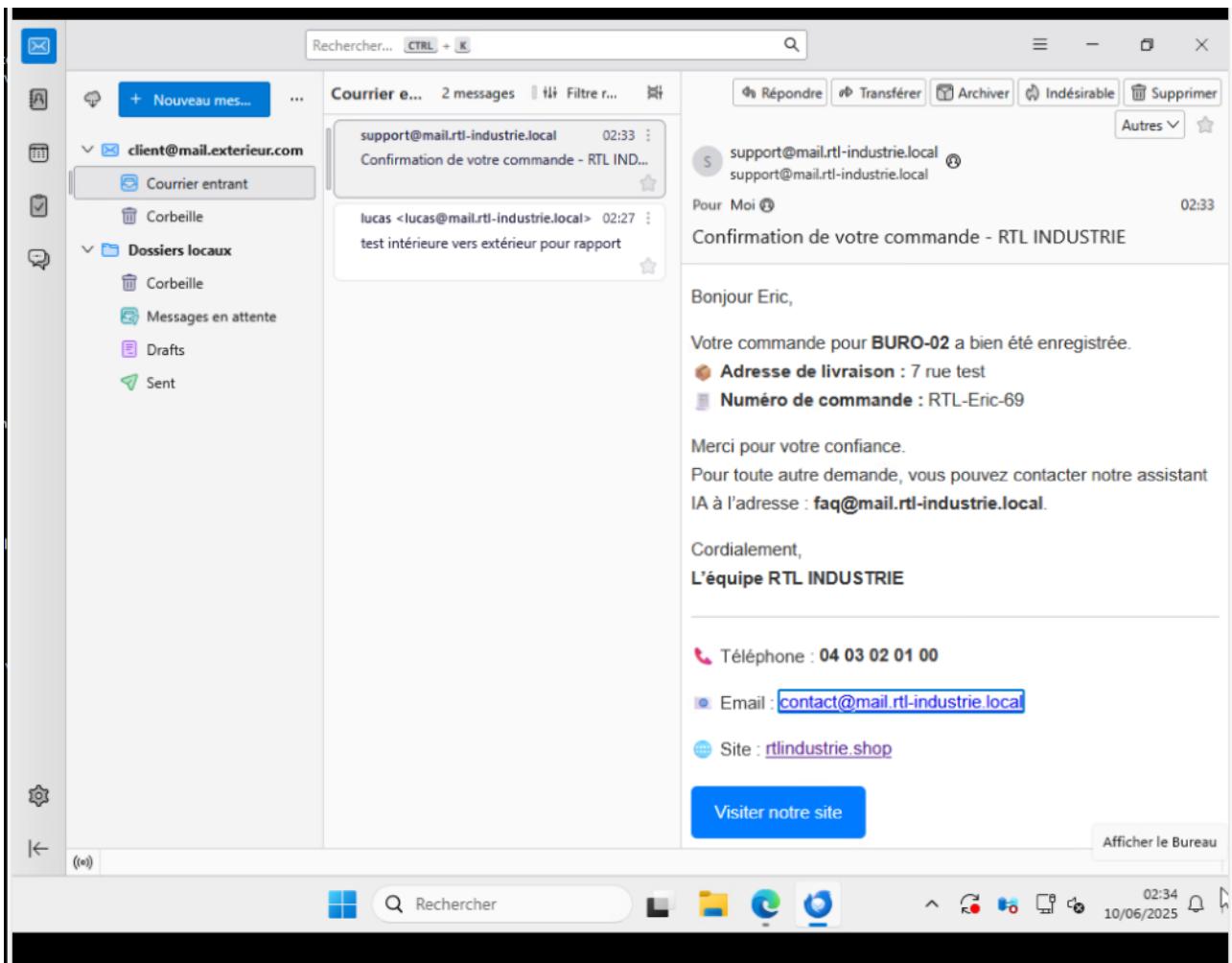
- **Send Email (Comptable)** :
 - Adresse : ralph@mail.rtl-industrie.local
 - Contenu :

Achat reçu sur le site
Produit : {{produit}}
Client : {{nom}}, {{email}}
Merci d'enregistrer l'opération.

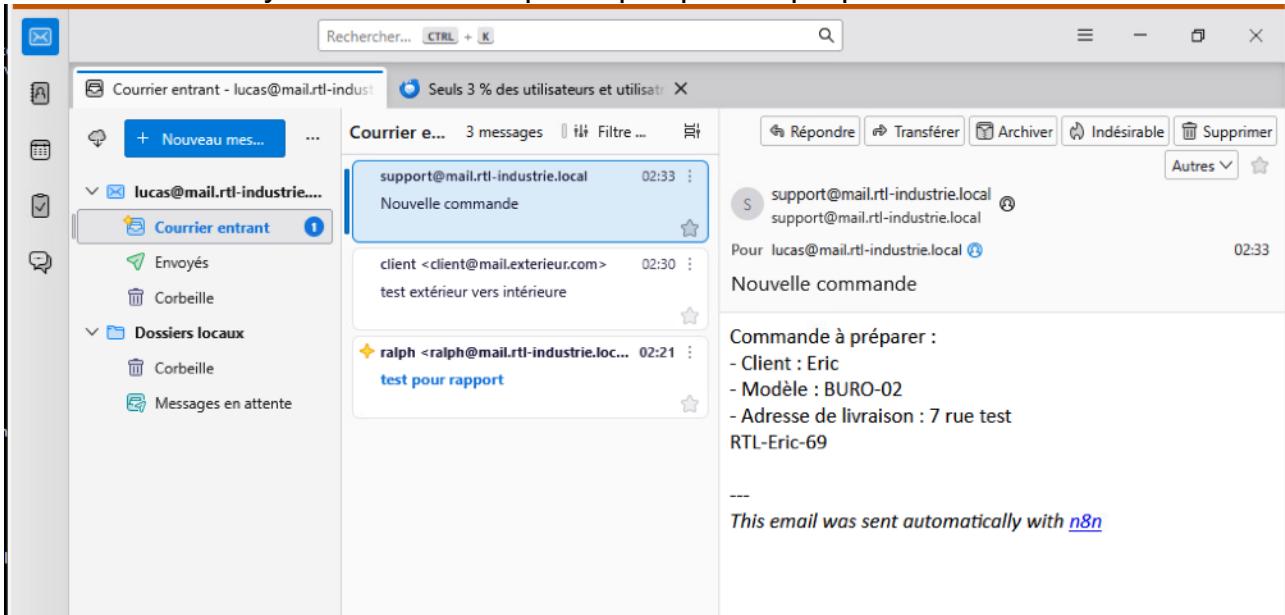
Le client achète sur le site:



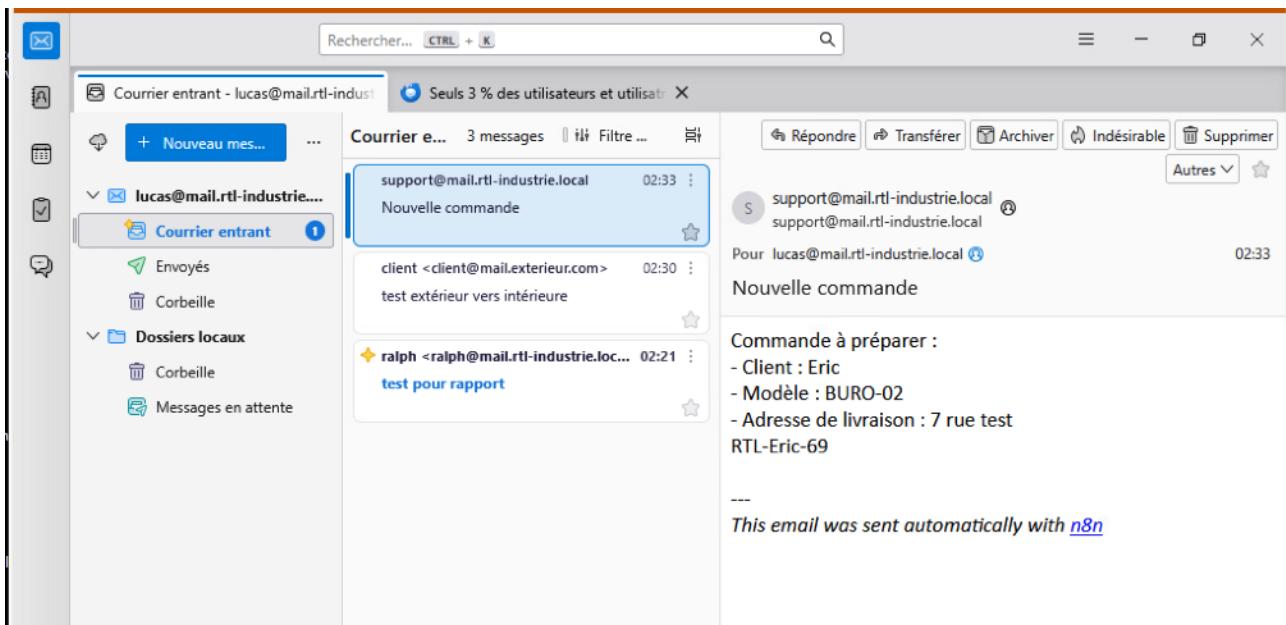
Un mail de confirmation lui ai envoyé:



Un mail est envoyé au technicien pour qu'il puisse préparer la commande:



Et au comptable pour qu'il puisse faire les comptes:



7. Résultat final

- Les 3 workflows sont testés et fonctionnels.
- Liaison validée avec le site rtl-industrie.shop.
- Les mails sont envoyés automatiquement depuis les bons comptes configurés.
- L'assistant IA améliore significativement la réactivité du support.