BTS Services informatiques aux organisations - SISR

Session 2022

E4 – Support et mise à disposition de services informatiques

Coefficient 4

DESCRIPTION DE LA REALISATION PROFESSIONNELLE

NOM et prénom du candidat :	

Contexte de la réalisation professionnelle

L'entreprise Les Ateliers De Joigny, dans une démarche de souveraineté numérique et d'éthique, a souhaité s'affranchir de sa dépendance aux solutions de messagerie propriétaires (GAFAM). L'objectif était de réduire les coûts liés aux licences récurrentes tout en conservant une solution collaborative performante et sécurisée.

Le besoin identifié était la mise en place d'un serveur de messagerie capable de s'intégrer à l'annuaire existant, de garantir une haute délivrabilité des mails et de proposer une interface utilisateur moderne. Cette évolution doit répondre aux exigences de sécurité actuelles (chiffrement, authentification centralisée, filtrage antispam).

La solution retenue est Grommunio, une alternative Open Source à Microsoft Exchange, pour sa compatibilité native avec les protocoles Outlook et sa facilité d'administration. Cette réalisation couvre le déploiement de l'appliance, l'interconnexion LDAP avec l'Active Directory, la configuration DNS avancée chez l'hébergeur IONOS et la sécurisation des flux via un Reverse Proxy Traefik.

Intitulé de la réalisation professionnelle

Mise en place d’un serveur mail

Période de réalisation : 03/2026 **Lieu : Joigny**
Modalité : Individuelle

Principale(s) activité(s) concernée(s) :

Développer la présence en ligne de l’organisation
Mettre à disposition des utilisateurs un service informatique

Conditions de réalisation

Ressources présentes (Avant la RP)

- **Infrastructure de virtualisation :** Serveur physique sous **VMware ESXi**.
- **Annuaire :** Contrôleur de domaine sous **Windows Server 2022** fonctionnel.
- **Réseau :** Segmentation par VLANs en place, accès internet via pare-feu.
- **Nom de domaine :** Domaine jjba.fr géré sur l'interface **IONOS**.
- **Service tiers :** Instance **Traefik** déjà déployée pour la gestion des certificats SSL et du routage HTTP/HTTPS.

Résultats attendus (Après la RP)

- **Service de messagerie :** Serveur Grommunio opérationnel et accessible via mail.jjba.fr.
- **Centralisation :** Synchronisation réussie des utilisateurs de l'**Active Directory** vers Grommunio via LDAP.
- **Délivrabilité :** Configuration optimale des enregistrements **MX, SPF, DKIM et DMARC** pour éviter les spams.
- **Accessibilité :** Accès sécurisé au Webmail et configuration automatique des clients (Autodiscover).

Durée de réalisation : Environ 15 heures (Installation, configuration LDAP, débogage DNS et tests de délivrabilité).

Modalités d'accès à cette réalisation professionnelle.

https://site.jjba.fr. Compte d'accès : aucun. Mot de passe : BTSsiosisr

Partie 1 – Procédure de mise en œuvre.

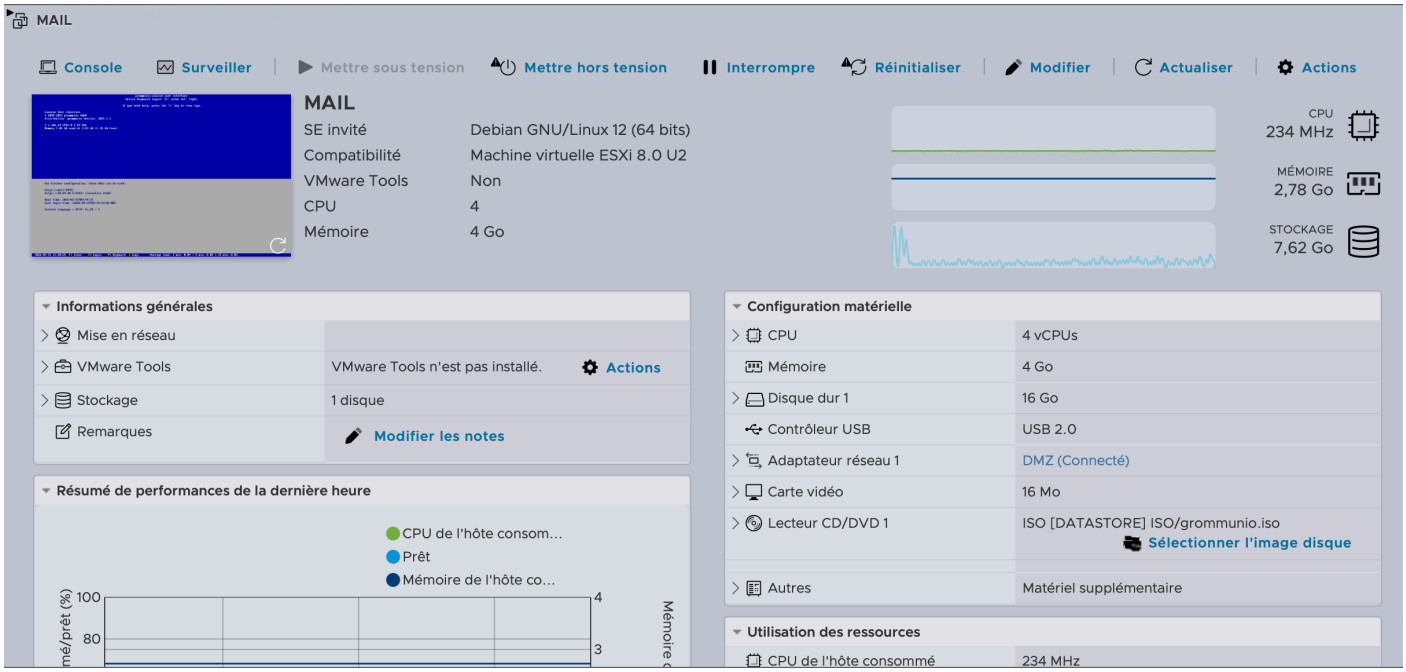
1. Liste des outils utilisés

- **Hyperviseur :** VMware ESXi 7.0
- **Système :** ISO Grommunio (Appliances basées sur openSUSE Tumbleweed)
- **Gestionnaire de paquets :** zypper
- **Annuaire :** Active Directory (Windows Server 2022)
- **Reverse Proxy :** Traefik (Docker)
- **Gestion DNS :** Interface d'administration IONOS
- **Tests :** Mail-Tester.com

2. Déploiement de l'infrastructure (Virtualisation)

La première étape consiste à créer la machine virtuelle sur l'ESXi.

- **Ressources :** 4 vCPU, 8 Go de RAM, 100 Go de disque.
- **Réseau :** Assignation au VLAN "SRV MAIL" (ID 40).
- **Installation :** Boot sur l'ISO et configuration de l'adresse IP statique via l'assistant de l'appliance.
    - IP LAN : 10.89.40.5
    - Hostname : mail.jjba.fr



3. Configuration du Reverse Proxy (Traefik)

Pour rendre le service accessible de l'extérieur en HTTPS (port 443), Grommunio est placé derrière Traefik.

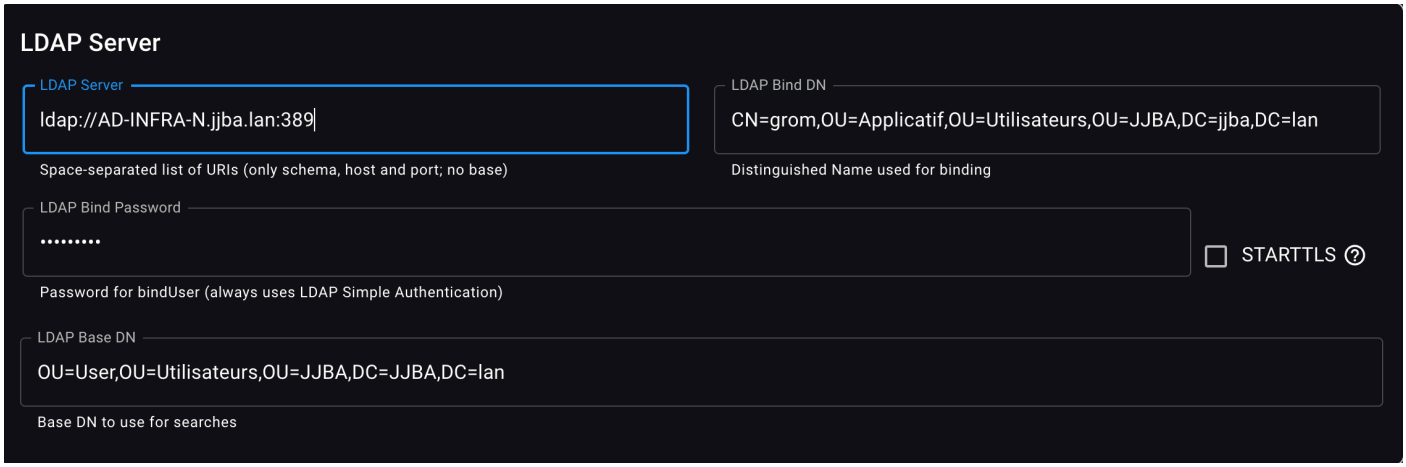
- Configuration du routage : Traefik intercepte les requêtes pour mail.jjba.fr.
- Redirection vers l'IP interne 10.89.40.5 sur le port 8443 (interface admin) et 443 (webmail).
- Génération du certificat SSL (Let's Encrypt) via Traefik.

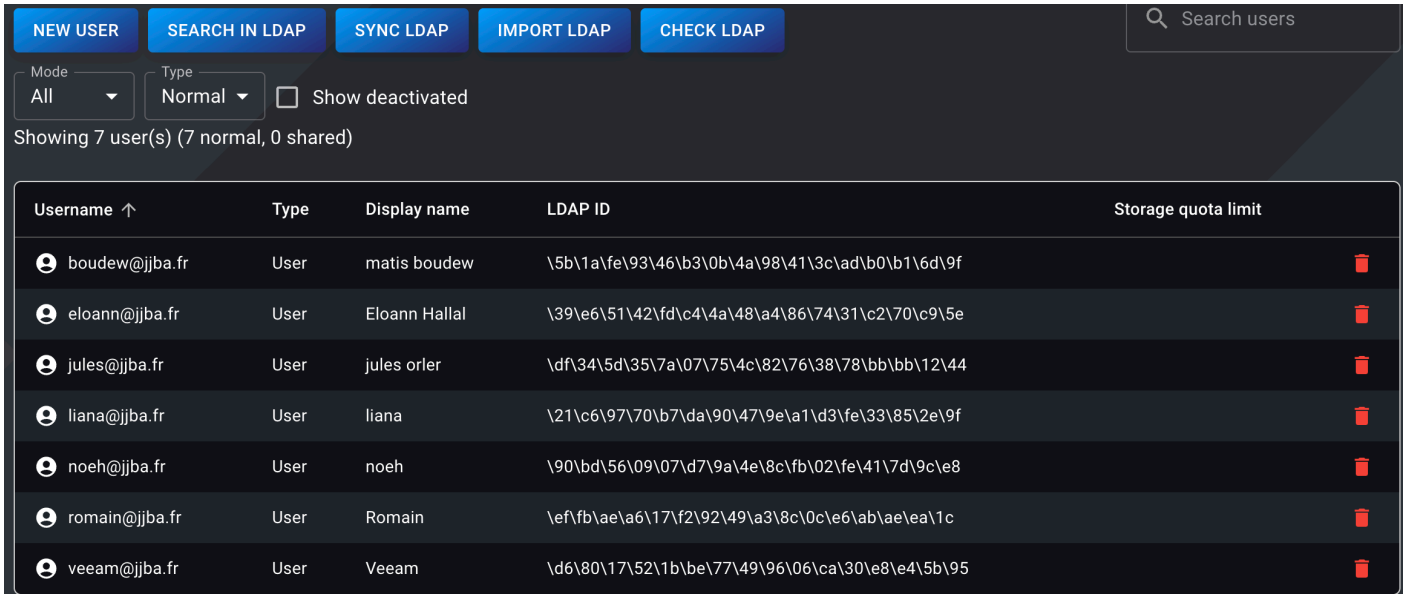
4. Interconnexion avec l'Active Directory (LDAP)

Pour centraliser la gestion des utilisateurs, nous lions Grommunio au serveur Windows Server 2022.

- **Configuration LDAP dans l'admin Grommunio :**
    - Hôte : IP du contrôleur de domaine.
    - Base DN : OU=Utilisateurs,DC=jjba,DC=fr
    - Filtre : Synchronisation basée sur l'attribut mail.

- **Action :** Importation des utilisateurs. Chaque utilisateur créé dans l'AD avec une adresse mail est automatiquement reconnu par Grommunio.





5. Configuration DNS et Sécurité (IONOS)

C'est l'étape cruciale pour garantir que nos mails ne finissent pas en SPAM. Nous configurons les enregistrements chez IONOS :

- **Enregistrement A :** mail.jjba.fr -> 5.196.216.188 (IP Publique).
- **Enregistrement MX :** Indique que mail.jjba.fr gère les mails du domaine.
- **Sécurisation SPF :** v=spf1 a mx ip4:5.196.216.188 -all (Autorise uniquement notre serveur à envoyer).
- **Configuration DKIM :** 1. Génération de la clé sur le serveur (via les outils openDKIM intégrés). 2. Ajout de l'enregistrement TXT default._domainkey sur IONOS avec la clé publique.
- **DMARC :** Mise en place d'une politique de quarantaine (p=quarantine).

☐	MX	@	mail.jjba.fr	-	✎ 🗑
☐	TXT	@	"v=spf1 a mx ip4:5.196.216.188 -all"	-	✎ 🗑
☐	TXT	_dmarc	"v=DMARC1; p=quarantine; rua=mailto:post...	-	✎ 🗑
☐	TXT	default._domainkey	"v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQE...	-	✎ 🗑
☐	SRV	_autodiscover._tcp	0 443 mail.jjba.fr	-	✎ 🗑
☐	CNAME	audi	jjba.fr	-	✎ 🗑
☐	CNAME	autoconfig	mail.jjba.fr	-	✎ 🗑
☐	CNAME	autodiscover	mail.jjba.fr	-	✎ 🗑

6. Administration en ligne de commande

Grommunio étant basé sur openSUSE, l'administration fine se fait en SSH.

- Mise à jour du système : zypper refresh && zypper update
- Vérification des services : systemctl status gromox-*

```
mail:~ # systemctl status gromox-*
● gromox-delivery-queue.service - Gromox local delivery agent frontend
     Loaded: loaded (/usr/lib/systemd/system/gromox-delivery-queue.service; enabled; preset: disable>
     Active: active (running) since Wed 2026-03-25 09:44:53 CET; 6 days ago
       Docs: man:delivery-queue(8gx)
   Main PID: 1663 (delivery-queue)
      Tasks: 6 (limit: 4669)
        CPU: 1min 37.265s
     CGroup: /system.slice/gromox-delivery-queue.service
             └─1663 /usr/libexec/gromox/delivery-queue

mars 25 09:44:53 mail gromox-delivery-queue[1663]: system: maximum file descriptors: 524288
mars 25 09:44:53 mail delivery-queue[1663]: gromox-delivery-queue 3.3.16.m985997b (pid 1663 uid 475)
mars 25 09:44:53 mail gromox-delivery-queue[1663]: system: host ID is "mail.jjba.fr"
mars 25 09:44:53 mail gromox-delivery-queue[1663]: system: rectified contexts number to 400
mars 25 09:44:53 mail gromox-delivery-queue[1663]: dq: STARTTLS support is off
mars 25 09:44:53 mail gromox-delivery-queue[1663]: dq: maximum mail length is 64M
mars 25 09:44:53 mail gromox-delivery-queue[1663]: system: maximum file descriptors: 524288
mars 25 09:44:53 mail gromox-delivery-queue[1663]: ldap_adaptor: default host <ldap://AD-INFRA-N.jjb>
mars 25 09:47:08 mail gromox-delivery-queue[1663]: remote=[::1] from=<no.envelope.from@invalid> to={>
mars 26 08:10:21 mail gromox-delivery-queue[1663]: remote=[::1] from=<toto@pllm.fr> to={noeh@jjba.fr>

● gromox-midb.service - Gromox midb service
     Loaded: loaded (/usr/lib/systemd/system/gromox-midb.service; enabled; preset: disabled)
     Active: active (running) since Wed 2026-03-25 09:44:53 CET; 6 days ago
       Docs: man:midb(8gx)
   Main PID: 1667 (midb)
      Tasks: 105 (limit: 4669)
        CPU: 2min 18.941s
     CGroup: /system.slice/gromox-midb.service
             └─1667 /usr/libexec/gromox/midb

mars 25 09:44:53 mail systemd[1]: Started Gromox midb service.
mars 25 09:44:53 mail midb[1667]: gromox-midb 3.3.16.m985997b (pid 1667 uid 0)
mars 25 09:44:53 mail gromox-midb[1667]: system: maximum file descriptors: 524288
mars 25 09:44:53 mail gromox-midb[1667]: system: defaulting to implicit access ACL containing ::1.
mars 25 09:44:53 mail midb[1667]: gromox-midb 3.3.16.m985997b (pid 1667 uid 475)
mars 25 09:44:53 mail gromox-midb[1667]: system: maximum file descriptors: 524288
mars 25 09:44:53 mail gromox-midb[1667]: system: defaulting to implicit access ACL containing ::1.
mars 25 09:44:53 mail gromox-midb[1667]: ldap_adaptor: default host <ldap://AD-INFRA-N.jjba.lan:389>>

● gromox-zcore.service - Gromox zcore service
     Loaded: loaded (/usr/lib/systemd/system/gromox-zcore.service; enabled; preset: disabled)
     Active: active (running) since Wed 2026-03-25 09:44:53 CET; 6 days ago
       Docs: man:zcore(8gx)
   Main PID: 1669 (zcore)
      Tasks: 18 (limit: 4669)
        CPU: 2min 29.377s
     CGroup: /system.slice/gromox-zcore.service
             └─1669 /usr/libexec/gromox/zcore

mars 25 09:44:53 mail systemd[1]: Started Gromox zcore service.
mars 25 09:44:53 mail zcore[1669]: gromox-zcore 3.3.16.m985997b (pid 1669 uid 0)
mars 25 09:44:53 mail gromox-zcore[1669]: system: maximum file descriptors: 524288
mars 25 09:44:53 mail gromox-zcore[1669]: system: SMTP server is sendmail://localhost
```

Partie 2 – Validation.

1. Test de flux sortant (Délivrabilité)
Pour vérifier la conformité de la configuration (SPF, DKIM, DMARC), j'ai utilisé l'outil **Mail-Tester**.

- **Action :** Envoi d'un mail depuis l'adresse noeh@jjba.fr vers l'adresse de test unique fournie par la plateforme.
- **Résultat :** Un score de **9/10** a été obtenu.
- **Analyse :** Le point manquant est lié à la "signature DKIM" qui, bien que présente et valide, peut parfois être interprétée différemment selon le format de la clé (1024 vs 2048 bits). Cependant, ce score garantit que les mails arrivent en "Boîte de réception" chez Gmail, Outlook, etc.

2. Test de flux entrant

Vérification de la bonne réception des messages externes sur le serveur Grommunio.

- **Action :** Envoi d'un mail depuis une adresse personnelle (noehaoudani@gmail.com) vers noeh@jjba.fr.
- **Constat :** Le mail est reçu instantanément dans le Webmail Grommunio. Cela valide le bon fonctionnement de l'enregistrement **MX** chez IONOS et du routage via le reverse proxy **Traefik**.

3. Validation de l'authentification AD/LDAP

Il est crucial de vérifier que les utilisateurs de l'entreprise peuvent se connecter avec leurs identifiants de session habituels.

- **Test :** Tentative de connexion sur l'interface https://mail.jjba.fr avec un compte créé dans l'Active Directory 2022.
- **Résultat :** L'authentification réussit, la boîte aux lettres est automatiquement provisionnée lors de la première connexion grâce à la synchronisation LDAP.

5. Test de l'Autodiscover

- **Action :** Configuration du compte mail sur un smartphone ou un client Outlook en saisissant uniquement l'adresse mail et le mot de passe.
- **Résultat :** Grâce aux enregistrements **SRV et CNAME** configurés chez IONOS, le client mail trouve automatiquement les paramètres du serveur sans saisie manuelle.

Partie 3 – Veille technologique.

1. Comparaison des solutions de messagerie

Avant de retenir **Grommunio**, plusieurs alternatives ont été étudiées pour répondre au besoin de souveraineté des Ateliers de Joigny :

- **Zimbra / Carbonio :** Solutions robustes mais très gourmandes en ressources RAM et complexes à mettre à jour en version Open Source.
- **Microsoft 365 / Google Workspace :** Solutions SaaS performantes mais exclues pour des raisons d'éthique, de coût de licence par utilisateur et de dépendance aux GAFAM.
- **Grommunio :** Choisi pour sa légèreté, son interface moderne et son intégration native du protocole RPC over HTTP (MAPI), permettant une compatibilité parfaite avec Microsoft Outlook sans plugin.

2. Évolution de la sécurité : La délivrabilité (DKIM/DMARC)

Lors de la réalisation, une veille spécifique a été faite sur le **DKIM (DomainKeys Identified Mail)**.

- **Recherche :** L'objectif était de comprendre comment signer numériquement les mails pour prouver qu'ils n'ont pas été altérés.
- **Amélioration possible :** Tester la rotation des clés DKIM (changer de clé tous les 6 mois) pour renforcer la sécurité. L'utilisation d'une clé de **2048 bits** au lieu de 1024 bits est également une piste pour atteindre le score de 10/10 sur Mail-Tester.

3. Protection contre le Spam et les Menaces

Bien que Grommunio intègre des outils de base (RSPAMD), une veille sur des passerelles de sécurité dédiées a été effectuée :

- **Proxmox Mail Gateway (PMG) :** Solution Open Source qui se place en amont du serveur de mail pour filtrer 99% des spams et virus avant qu'ils n'atteignent Grommunio.
- **SpamAssassin :** Étude des règles de filtrage personnalisées pour bloquer les tentatives de phishing ciblées sur l'entreprise.

4. Authentification et Protocoles

- **LDAPS :** Pour la suite, une veille est menée sur le passage du LDAP classique vers le **LDAPS (LDAP over SSL)** sur le port 636 pour chiffrer les échanges entre l'AD 2022 et Grommunio.
- **MFA (Multi-Factor Authentication) :** Étude de l'implémentation de la double authentification pour l'accès au Webmail afin de sécuriser les comptes contre le vol de mots de passe.

Liens de veille (Exemples à citer à l'oral ou mettre en annexe) :

- *Documentation officielle Grommunio :* https://docs.grommunio.com/
- *Sécurité des emails (ANSSI) :* Guide sur les bonnes pratiques de configuration SPF/DKIM/DMARC.
- *Outil de test :* https://www.mail-tester.com/