CHECKLIST IMPRIMABLE

Votre feuille de route pour un serveur Matrix privé, fiable et maîtrisé

Préparez, déployez et sécurisez votre instance Matrix dans le bon ordre. Cochez chaque point avant de passer à l'étape suivante : un serveur fermé et restaurable est une meilleure base qu'une ouverture précipitée.

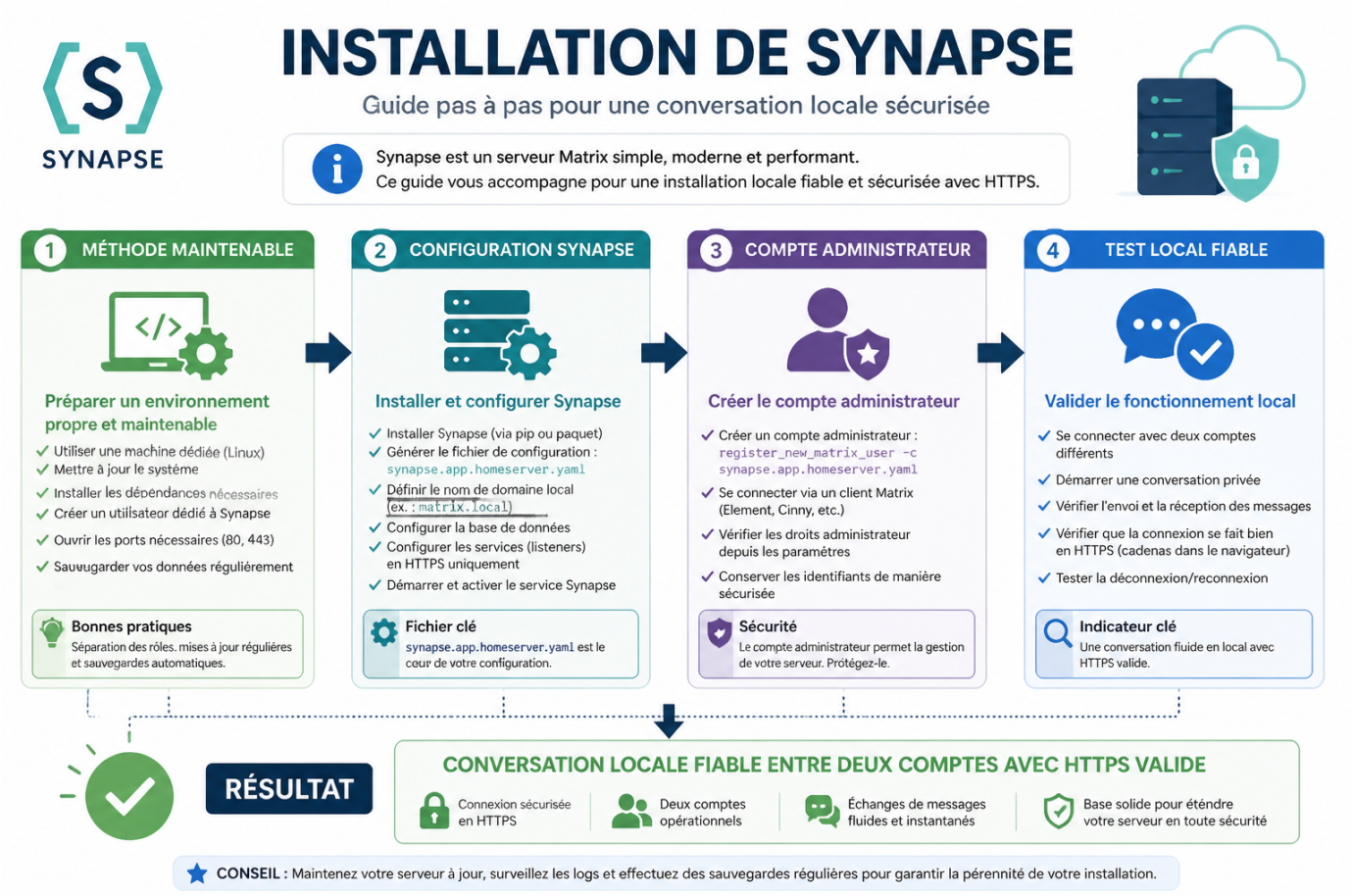
Au sommaire

Les 3 rôles à distinguer

Matrix est le protocole : il définit les règles de communication entre clients et serveurs compatibles.

Element est un client : il permet aux utilisateurs de se connecter, mais n'est pas le seul client Matrix possible.

Synapse est le serveur : il héberge les comptes, les salons et les données de service de votre instance.



INFOGRAPHIE *Étapes d'installation Synapse pour créer un serveur Matrix privé*

1. Préparer une base technique durable

Choisir une machine virtuelle Linux ou un serveur dédié administrable.
Privilégier une adresse réseau stable et un stockage persistant.

Définir un périmètre de départ limité.
Quelques comptes, des salons privés et aucune inscription publique au lancement.

- [ ] **Prévoir un espace de sauvegarde séparé du serveur.**
  Une copie sur le même disque ne protège pas contre tous les incidents.
- [ ] **Consulter la documentation officielle de Matrix et de Synapse avant d'exécuter les commandes.**
  Les méthodes d'installation, options et chemins de configuration évoluent.

2. Valider domaine, DNS et accès système

- [ ] **Réserver un nom de domaine ou sous-domaine dédié à l'instance.**
  Il fera partie des identifiants Matrix, par exemple @pseudo:serveur.
- [ ] **Configurer l'enregistrement DNS vers l'adresse IP du serveur.**
- [ ] **Vérifier la résolution DNS avant de déployer le service.**
  HTTPS et les communications avec des clients distants en dépendent.
- [ ] **Créer un accès d'administration distinct de l'usage quotidien.**
- [ ] **Appliquer les mises à jour de sécurité du système et utiliser une authentification forte pour l'administration.**
  Une clé SSH, des comptes autorisés limités et un pare-feu adapté constituent une base utile.

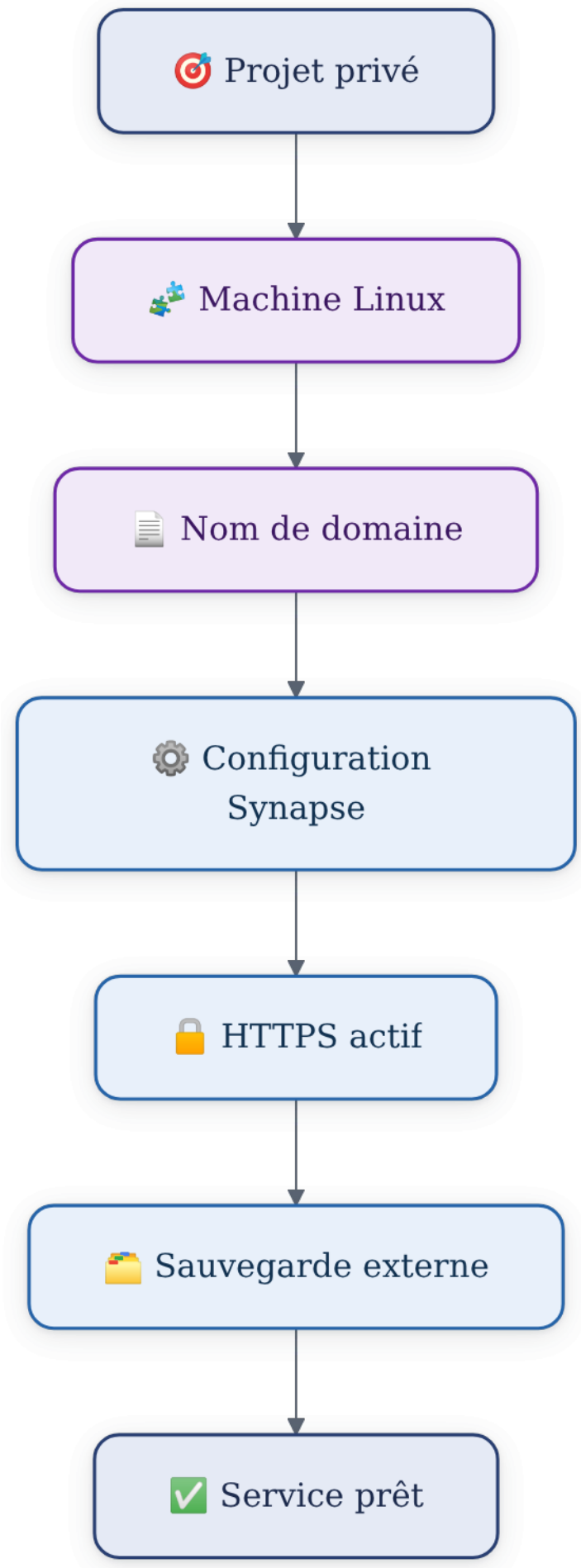

🎯 Projet privé
🧩 Machine Linux
📄 Nom de domaine
⚙️ Configuration Synapse
🔒 HTTPS actif
🗂️ Sauvegarde externe
✅ Service prêt

SCHÉMA *Les briques à relier : hébergement Linux, Synapse, HTTPS et sauvegarde séparée.*

3. Déployer Synapse sans ouvrir trop vite

- [ ] **Installer Synapse avec une méthode maintenue par l'éditeur ou la distribution Linux.**
- [ ] **Générer la configuration initiale avec le nom de domaine choisi.**
- [ ] **Activer HTTPS avec un certificat TLS valide.**
  Prévoir aussi le suivi de son renouvellement.
- [ ] **Créer le premier compte administrateur avant d'inviter d'autres utilisateurs.**
- [ ] **Désactiver ou restreindre l'inscription publique.**
  La création de comptes par l'administrateur réduit l'exposition initiale au spam et aux erreurs.
- [ ] **Créer un salon de test et vérifier la connexion depuis un client compatible, tel qu'Element.**

4. Contrôler sécurité, chiffrement et sauvegardes

- [ ] **Vérifier les appareils utilisés pour les conversations chiffrées de bout en bout.**
  Le chiffrement ne dispense pas de la vérification des appareils.
- [ ] **Prévoir la sauvegarde des clés de chiffrement.**
  Sans cette préparation, l'accès à l'historique chiffré peut devenir difficile après un changement d'appareil.
- [ ] **Sauvegarder les données importantes du serveur et sa configuration.**
- [ ] **Tester une restauration.**
  Une sauvegarde n'est réellement utile que si sa restauration a été vérifiée.
- [ ] **Documenter les accès d'administration, les règles d'inscription et la procédure de récupération.**
- [ ] **Prévoir les mises à jour et une supervision régulière de l'instance.**

> ! **À retenir avant d'activer la fédération**
> La fédération Matrix peut être envisagée après validation du fonctionnement de base. Commencez par maîtriser les comptes locaux, les salons privés, HTTPS, les sauvegardes et la restauration : l'ouverture immédiate au réseau n'est pas une obligation.

Le chiffrement de bout en bout protège le contenu des conversations compatibles, mais les métadonnées techniques, les journaux, les sauvegardes et les appareils non vérifiés demandent aussi une gestion attentive.