CHECKLIST IMPRIMABLE

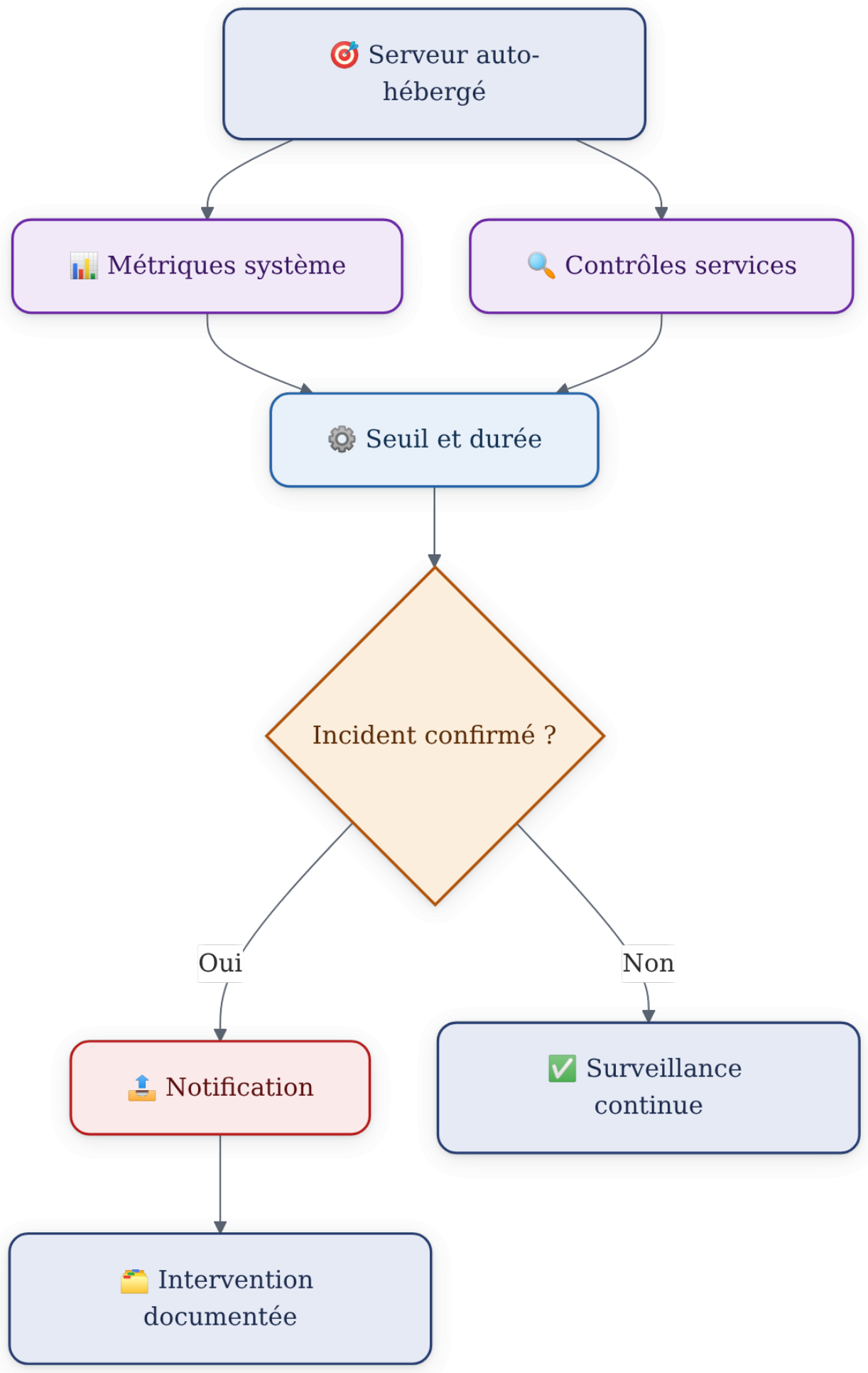
Ma checklist de supervision : serveur, services et alertes

Mettez en place une surveillance utile sans multiplier les métriques ni les notifications inutiles. Cette fiche vous aide à protéger d'abord les services qui comptent réellement.

Au sommaire

1. Identifier ce qui doit rester disponible

- [ ] **Lister les services dont l'arrêt a un impact concret**
  Par exemple : site web, API, fichiers, base de données, VPN, relais mail ou application métier.
- [ ] **Noter pour chaque service l'adresse, l'URL ou le port à contrôler**
- [ ] **Identifier la dépendance principale de chaque service**
  Exemple : un site peut dépendre du serveur web, de la base de données et du stockage.
- [ ] **Définir le responsable et la réaction attendue en cas d'alerte**
- [ ] **Limiter la première liste aux services réellement critiques**
  Une courte liste priorisée est plus exploitable qu'une couverture exhaustive sans priorité.


🎯 Serveur auto-hébergé
📊 Métriques système
🔍 Contrôles services
⚙️ Seuil et durée
Incident confirmé ?
Oui
Non
📤 Notification
✅ Surveillance continue
🗂️ Intervention documentée

INFOGRAPHIE *Schéma de surveillance serveur auto-hébergé avec métriques, contrôles de services et alertes*

2. Poser le socle de mesures système

- [ ] **Surveiller le CPU et la charge système**
  Rechercher une charge élevée qui dure, plutôt qu'un pic isolé.
- [ ] **Suivre la mémoire vive et l'usage du swap**
  La mémoire utilisée seule ne suffit pas toujours à caractériser un incident.
- [ ] **Contrôler l'espace disque et les inodes**
  Vérifier notamment les journaux, sauvegardes locales et volumes de conteneurs.
- [ ] **Observer le réseau, la latence et les erreurs d'interface**
- [ ] **Prévoir l'accès aux journaux système et applicatifs**
  Ils donnent le contexte lorsqu'une métrique ou un contrôle échoue.

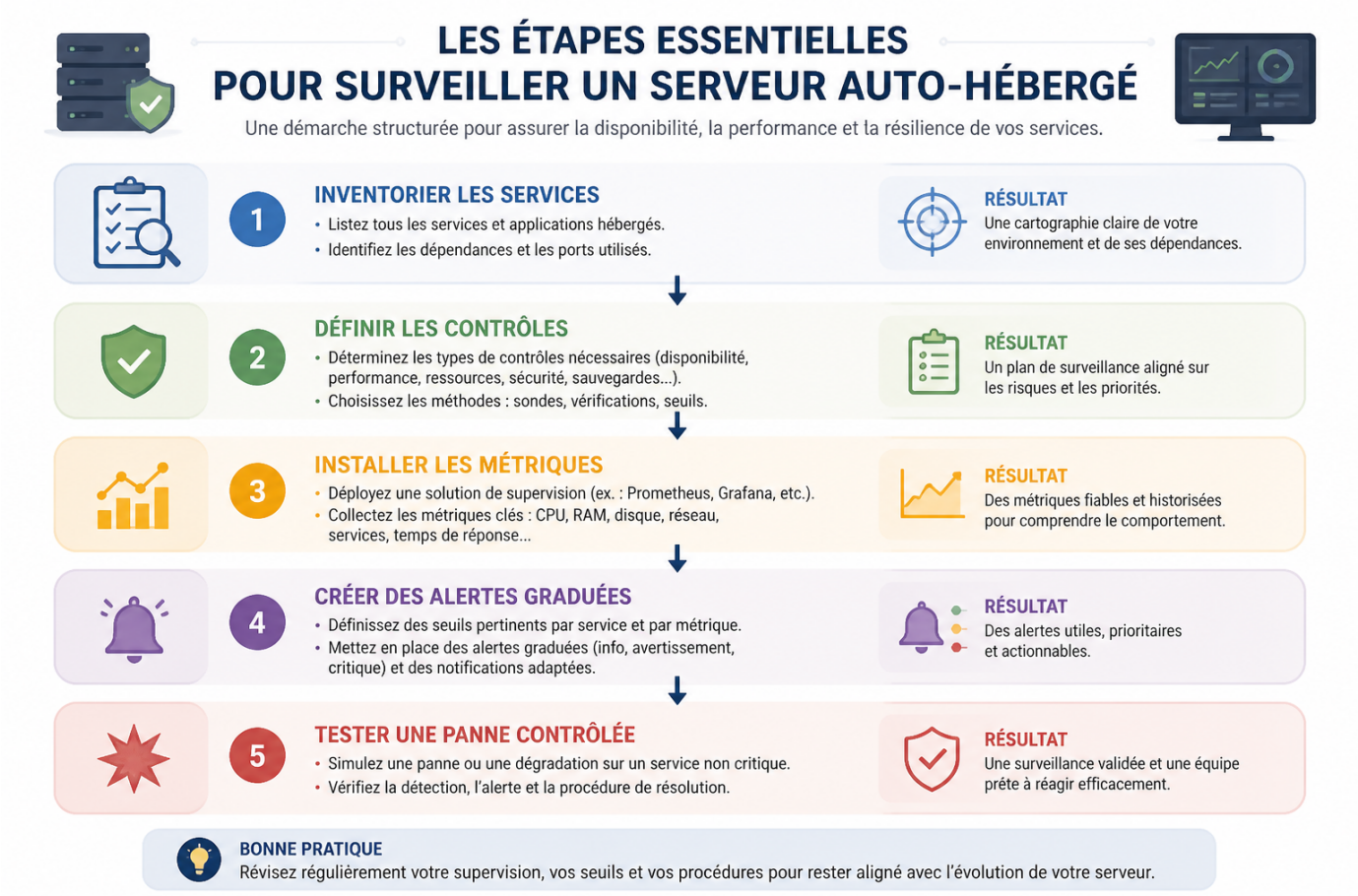


SCHÉMA *Les cinq étapes d'une supervision cohérente, de la mesure à l'alerte.*

3. Vérifier le service rendu, pas seulement la machine

- [ ] **Créer un contrôle de disponibilité pour chaque endpoint ou port critique**
- [ ] **Tester les services selon leur usage réel**
  HTTP(S), TCP, DNS, SSH, base de données, conteneur ou processus applicatif selon le besoin.
- [ ] **Vérifier le code HTTP ou le comportement applicatif attendu lorsque c'est pertinent**

- [ ] **Ne pas se contenter d'un ping**
  Un serveur peut répondre au réseau alors que le site, le reverse proxy ou la base de données est dégradé.
- [ ] **Ajouter un contrôle depuis une machine ou un site distinct lorsque l'enjeu le justifie**
  Une mesure locale ne peut pas alerter si le serveur est arrêté ou isolé du réseau.

4. Choisir une première combinaison d'outils libres

Besoin	Outil à envisager	Point d'attention
Vue immédiate des métriques d'un hôte	Netdata	Le stockage historique et les alertes demandent un paramétrage adapté.
Contrôles simples d'URL, ports ou DNS	Uptime Kuma	Complète les métriques ; ne les remplace pas.
Historique, requêtes et tableaux de bord pour plusieurs services ou hôtes	Prometheus + Grafana	Prévoir les exports, les règles et le stockage.
Supervision centralisée d'un parc hétérogène	Zabbix	Le déploiement est plus structurant pour un serveur seul.

5. Rendre chaque alerte exploitable

- [ ] **Formuler l'alerte autour d'un symptôme précis**
  Éviter les messages vagues qui ne permettent pas de décider quoi faire.
- [ ] **Commencer avec des seuils d'observation plutôt que des seuils de panique**
- [ ] **Détecter une saturation durable, pas seulement une valeur ponctuelle**
- [ ] **Prévoir une alerte de capacité pour un disque qui se remplit durablement**
- [ ] **Prévoir une alerte de performance si le temps de réponse reste anormal pendant plusieurs contrôles**
- [ ] **Associer chaque notification à une décision**
  Observer, libérer de l'espace, redémarrer un service, appliquer une procédure de secours ou ouvrir un incident.

> ! **Ne masquez pas les indices**
> Évitez les redémarrages précipités : consultez d'abord les journaux et le contexte de l'alerte. Redémarrer sans diagnostic peut effacer les éléments nécessaires à la compréhension de l'incident.

6. Tester et sécuriser le dispositif

- [ ] **Simuler une panne contrôlée d'un service critique**
- [ ] **Vérifier que le contrôle local détecte le problème**
- [ ] **Vérifier que le contrôle externe détecte aussi l'indisponibilité**
- [ ] **Confirmer la réception de la notification et la clarté de sa consigne**
- [ ] **Restreindre l'interface de supervision aux administrateurs autorisés**
- [ ] **Protéger l'accès avec chiffrement, contrôle d'accès et mises à jour régulières**

La supervision complète les sauvegardes et le plan de restauration ; elle ne les remplace pas.