Plan de supervision

1. Objectifs de la supervision

- Garantir la disponibilité et la performance des services critiques (AD, DNS, DHCP, fichiers, messagerie, ERP).
- Détecter rapidement les incidents grâce à une surveillance en temps réel.
- Assurer le suivi des actions correctives et la traçabilité via GLPI.

2. Cibles de supervision

- Infrastructures serveurs (physiques et virtualisés Proxmox/VMware)
- Réseau : switches, VLANs, VPN IPsec/WireGuard, firewall pfSense
- Services système : Active Directory, DNS, DHCP, services d'impression
- Applications clés : Serveurs de fichiers, messagerie, ERP
- Outils de sécurité : IDS/IPS, antivirus, gestion des correctifs
- Sauvegardes : état, fréquence, réussite

3. Outils et technologies

- Zabbix ou Centreon pour la collecte, alertes et tableaux de bord
- GLPI pour gestion des tickets incidents et inventaire
- Intégration des logs dans un SIEM pour analyse avancée (optionnel)
- Supervision des performances système (CPU, RAM, Disk I/O, latence)

4. Paramètres surveillés et seuils

- Disponibilité services critiques : ICMP, ports spécifiques (LDAP, SMB, SMTP, etc.)
- Performance serveur : charge CPU < 75%, mémoire libre > 20%, espace disque > 15%
- Utilisation bande passante et état des liens VPN/fibre
- État des backups : réussite/échec, temps d’exécution
- Tentatives et alertes sécurité : connexions suspectes, modifications non autorisées

5. Processus d’alerte et d’escalade

- Notification immédiate via emails/SMS aux équipes support pour alertes critiques
- Escalade en cas de non-réponse sous 15 min
- Reporting quotidien des incidents et résolutions
- Revue hebdomadaire des tendances et ajustement des seuils

6. Documentation et formation

- Guides d’utilisation des outils de supervision
- Procédures de gestion des incidents et bascule PRA
- Formation continue des équipes IT multisites