

# Mise en œuvre de la supervision des infrastructures

---

## 8.1. Introduction à la supervision

La supervision consiste à **surveiller en continu l'état de santé, la performance, la disponibilité et la sécurité des infrastructures IT**. Elle est essentielle au **Maintien en Condition Opérationnelle (MCO)**, à la **prévention des incidents**, à la **réduction des temps d'intervention**, et à la **traçabilité des anomalies**.

### Objectifs :

- Anticiper les dégradations de service
  - Être alerté en temps réel d'une panne ou anomalie
  - Centraliser les métriques, événements, et logs
  - Aider au diagnostic post-incident
  - Fournir des rapports de performance
- 

## 8.2. Architecture de supervision

### Composants d'une architecture :

- **Collecteurs** (agents, sondes) : remontent les données (Zabbix agent, SNMP, etc.)
- **Serveur de supervision** : traite les données, génère des alertes
- **Base de données** : stocke l'historique
- **Interface Web** : tableau de bord, reporting, visualisation
- **Notifications** : mails, SMS, webhook, Discord, etc.

### Types de supervision :

- Supervision **technique** (CPU, RAM, disque, réseau)
  - Supervision **applicative** (web, base de données, authentification)
  - Supervision **de sécurité** (ports ouverts, logs suspects, IDS)
  - Supervision **métier** (indicateurs SLA, taux de réussite...)
- 

## 8.3. Solutions de supervision

### Outils open source :

| Outil  | Fonction  |
|--------|---|
| Zabbix | Supervision complète, notifications, graphiques |

| Outil                  | Fonction                                   |
|------------------------|--|
| Centreon               | Interface claire, modèles prêts à l'emploi |
| Prometheus + Grafana   | Métriques temps réel, dashboards           |
| Nagios / Icinga        | Historique, simplicité, scripts            |
| GLPI + FusionInventory | Parc + supervision de base                 |
| Wazuh / OSSEC          | Supervision sécurité et logs               |

#### Outils commerciaux :

- PRTG
- SolarWinds
- Dynatrace
- NewRelic

## 8.4. Mise en place d'un serveur de supervision (ex. Zabbix)

#### Étapes clés :

1. Préparation du serveur (VM dédiée, Linux Ubuntu/CentOS)
2. Installation de la base de données (MySQL, PostgreSQL)
3. Déploiement de l'interface Web (Apache/Nginx)
4. Configuration des agents (Zabbix Agent sur chaque machine)
5. Ajout d'hôtes, modèles, alertes

#### Bonnes pratiques :

- Segmenter le trafic de supervision
- Sécuriser les connexions agent/serveur (certificats, ports)
- Utiliser des modèles standardisés (Linux, Windows, SNMP)

## 8.5. Collecte et gestion des métriques

#### Types de métriques à suivre :

- Charge CPU, RAM, espace disque
- Bande passante, erreurs réseau
- Disponibilité des services (ping, HTTP, ports)
- Temps de réponse applicatifs
- Statuts RAID, alimentation, température (via SNMP)

### Agrégation :

- Moyennes, seuils, minimum/maximum
  - Corrélations inter-hôtes
- 

## 8.6. Alertes et notifications

Les alertes doivent être **fiables, filtrées, hiérarchisées**.

| Niveau          | Exemple                      | Réaction                 |
|-----------------|------------------------------|--------------------------|
| <b>Info</b>     | Nouveau périphérique détecté | Consulter                |
| <b>Warning</b>  | Disque à 80%                 | Préparer action          |
| <b>Critical</b> | Perte de service réseau      | Intervenir immédiatement |

### Canaux :

- Email
  - SMS (gateway)
  - Webhook (Slack, Discord, Teams)
  - API (connexion outils ITSM)
- 

## 8.7. Visualisation et reporting

Les tableaux de bord (dashboards) sont indispensables pour :

- Afficher en temps réel l'état du SI
- Suivre les KPIs définis (taux de disponibilité, SLA)
- Analyser des périodes passées (baisse de performance)
- Présenter les résultats à la direction

### Outils recommandés :

- **Grafana** : visualisation avancée
  - **Zabbix UI / Centreon Web** : intégrés
  - **ELK Stack (Elasticsearch, Logstash, Kibana)** : logs + visualisation
- 

## 8.8. Supervision sécurité et conformité

La supervision est un **levier clé pour la cybersécurité** :

- Détection de ports ouverts non conformes
- Analyse des journaux (SIEM léger)
- Alertes en cas de brute force, accès suspect
- Suivi des politiques GPO

- Intégration Wazuh/OSSEC : détection des comportements anormaux

**Alignement avec ANSSI :**

- Journalisation horodatée
  - Ségrégation des flux critiques
  - Monitoring des comptes à privilèges
- 

## **8.9. Maintenance et évolution du système de supervision**

L'AIS doit :

- Mettre à jour régulièrement les outils
  - Revoir les seuils d'alerte
  - Tester les mécanismes de notification
  - Intégrer les nouveaux équipements
  - Documenter toute modification
  - Former ses collègues à l'interprétation des alertes
- 

## **8.10. Études de cas et évaluation**

**Projets pédagogiques :**

- Installation complète de Zabbix ou Centreon
- Supervision d'un réseau multi-VLAN
- Création d'un tableau de bord Grafana
- Alerte sur taux d'échec d'authentification

**Évaluations :**

- QCM supervision / métrologie / sécurité
- Étude de cas : mise en place supervision + documentation
- Oral : analyse d'un incident détecté par supervision