

PLATEFORME DE SUPERVISION INFOGÉRANCE

Fiche Synthétique Projet & Document Technique D'exploitation

- Linux Systemd
- Expérience Professionnelle (Intérim)
- Python / SNMP / WinRM
- PHP / MariaDB

Note : Ce document synthétise une réalisation technique professionnelle effectuée en entreprise, toutes les données sensibles (IPs, mots de passe, communautés SNMP) ont été anonymisées.

1. ARCHITECTURE & FONCTIONNEMENT GLOBAL



2. SCRIPTS DE COLLECTE AUTONOMES (PYTHON)

Cible	Technologie / Protocole	Métriques / Données Collectées	Localisation Script
Switchs Network (Alcatel-Lucent)	SNMP v2c (MIB-II & OIDs Propriétaires)	Uptime, état des ports (UP/DOWN), CPU, RAM, Température châssis	collector/switch/scanner.py
Serveurs Windows	WinRM (TCP 5985) + PowerShell CIM	Test ouverture socket, usage CPU, RAM, espace disque disponible	collector/server/scanner.py
Firewall FortiGate	SNMP v2c (MIB Fortinet)	Charge CPU/RAM, Tunnels IPsec (Phases 1/2), Sessions & IPs VPN SSL	collector/firewall/scanner.py

3. MATRIX DES ALERTES & SEUILS DE SUPERVISION

Seuils Matériels & Réseau (Firewall / Serveurs)			Supervision Applicative Web (cron_web.php)	
Statut	Conditions	Action Système	Chaque site web est évalué selon un score de santé (3 points max) :	
OK	CPU & RAM < 70%	Levée de l'alerte	• Disponibilité HTTP/HTTPS : Code de retour 200 à 399.	
WARNING	CPU ou RAM entre 70% et 84%	Création / MaJ alerte	• Validité SSL : Date d'expiration TLS > heure courante.	
CRITICAL	Injoignable OU CPU/RAM ≥ 85%	Alerte + Log incident	• Intégrité Contenu : Présence d'un mot-clé métier cible.	

4. AUTOMATISATION & EXPLOITATION SYSTÈME (LINUX)

Gestion des Daemons (Systemd)

Les scripts Python tournent en services d'arrière-plan résilients (`Restart=always` , `RestartSec=5s`).

```
# Vérifier le statut des services de collecte
sudo systemctl status switch server firewall

# Consulter les journaux d'exécution en temps réel
sudo journalctl -u switch -f

# Recharger la configuration après modification du service
sudo systemctl daemon-reload && sudo systemctl restart switch
```

Planification & Messagerie (Cron & SMTP)

- **Tâche Planifiée Web** : Exécution toutes les 5 min via crontab `* / 5 * * * * /usr/bin/php /var/www/html/cron_web.php`
- **File d'attente Mails** : Moteur asynchrone PHP avec gestion des priorités (Alertes immédiates vs Rapports différés) et support TLS (ports 587/465).

5. MATRICE DES FLUX RÉSEAU

Port	Protocole	Source → Destination	Usage / Description
161 / UDP	SNMP v2c	Serveur Supervision → Equipements (Switch, FW)	Collecte des métriques d'infrastructure (CPU, Ports, Tunnels)
5985 / TCP	WinRM HTTP	Serveur Supervision → Serveurs Windows	Vérification système et requêtes PowerShell CIM
80 / 443 / TCP	HTTP / HTTPS	Serveur Supervision → Sites Web Externe	Contrôle de réponse HTTP et validation certificats SSL
3306 / TCP	MySQL	Local / Internal	Stockage MariaDB des métriques, utilisateurs et alertes
587 / 465 / TCP	SMTP / STARTTLS	Serveur Supervision → Relais Mail	Envoi des alertes et rapports par courriel

6. SÉCURITÉ & SYNTHÈSE

Mesures de Sécurité

- Hachage fort des mots de passe (`create_user.php`).
- Contrôle d'accès basé sur les rôles (Admin / User).
- Externalisation des identifiants (`windows.conf` en `chmod 600`).
- Filtrage et assainissement des entrées PHP.

Compétences Valorisées

- **Système & Réseau** : Supervision réseau, protocoles (SNMP/WinRM), automatisation Systemd.
- **Développement** : Scripts Python/PHP, architecture BDD MariaDB, API JSON.
- **Exploitation** : Maintien en condition opérationnelle, documentation et procédures.