

Manuel des Bonnes Pratiques : Supervision, Sécurité et Organisation du Système de Fichiers Linux

PARTIE I – INSTALLATION MANUELLE VS APT : /opt/ ou apt ?

Critère	apt (apt install)	Installation manuelle dans /opt/
Mise à jour automatique	✓ Oui via <code>apt upgrade</code>	✗ Manuelle
Dépendances gérées automatiquement	✓ Oui	✗ À surveiller manuellement
Propreté système (isolation)	✗ S'installe globalement (ex: /usr/bin/, /etc/, /var/lib/)	✓ Auto-contenu dans /opt/
Personnalisation des versions	✗ Limité à celles dans les dépôts officiels	✓ Totale (dernières versions, flags compilés)
Contrôle de démarrage et debug	Intermédiaire (fichiers dispersés)	✓ Plein contrôle via scripts & systemd
🔥 Conflits potentiels	⚠ Possible si apt cohabite avec /opt/ versions	✗ Aucun si bien isolé

Recommandations

- Utilise `/opt/<app>` pour :
 - **Prometheus, Grafana, Blackbox, Node Exporter** (versions stables récentes)
 - Scripts binaires auto-maintenus
- Réserve **apt** pour :
 - Librairies système (**libssl, python3-pyinotify...**)
 - Services critiques sécurisés (**Fail2Ban, Wazuh, Suricata**)

PARTIE II – INSTALLATION SÉCURITÉ POUR TESTS DE CHARGE

1. Fail2Ban

- Rôle : bloque les tentatives de **brute-force** SSH ou HTTP.
- Installation :
`cd : sudo apt install fail2ban`
`cd : sudo systemctl enable --now fail2ban`
- Fichier de configuration principal : `/etc/fail2ban/jail.local`

Bonnes pratiques :

- Crée un filtre pour chaque exporter/port sensible.
- Intègre les logs `/var/log/auth.log`, `/var/log/nginx/error.log`.

2. Wazuh (SIEM léger)

- **Rôle** : analyse comportementale, collecte centralisée, **détection d'anomalies système/app**.
- Installation (agent sur ton instance) :
`cd : curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh`
`cd : bash ./wazuh-install.sh --agent`
- Connexion au serveur (préexistant ou Infomaniak si activé)
- Vérifie : `/var/ossec/logs/ossec.log`

Bonnes pratiques :

- Surveillance active des fichiers `/etc/prometheus/*`, `/opt/prometheus/*`
- Liens entre **telegraf/suricata/fail2ban** via logs.

3. Suricata (IDS/IPS réseau)

- **Rôle** : détecte **tentatives d'intrusion réseau**, scans, exfiltration
- Installation :
`cd : sudo apt install suricata`
`cd : sudo systemctl enable --now suricata`
- **Vérifie** :
`cd : sudo suricata -T -c /etc/suricata/suricata.yaml`
`cd : tail -f /var/log/suricata/fast.log`

Bonnes pratiques :

- Règles personnalisées selon l'usage Jitsi / exporters (trafic HTTP/ICMP/DNS/SSH)
- Active les logs JSON pour analyse Grafana.

Structure de dossier recommandée

```
/opt/  
├── prometheus/  
├── node_exporter/  
├── blackbox_exporter/  
├── grafana/  
├── monitoring/  
│   ├── Makefile_boot  
│   ├── Makefile_tasks  
│   ├── scripts/  
│   └── logs/
```

Commandes utiles à répéter (via cron ou `.bashrc`)

`cd /opt/monitoring && make start && make check`