05 - Maintenance et métrologie sur serveurs Linux

Objectif

- Montrer que l'administration avancée commence par l'observation : logs, intégrité et métriques système.

1. Pourquoi journaliser ?

> Les logs sont la mémoire opérationnelle du système.

1. Pourquoi journaliser ?

- Un système Linux exécute de nombreux sous-systèmes : noyau, services, tâches planifiées, réseau, authentification, applications.
- Les logs servent à vérifier que tout va bien, auditer, diagnostiquer, détecter une saturation ou comprendre un incident.

2. syslog

> Syslog est un format et un mécanisme de transmission de messages d'événements.

2. syslog

- Un message syslog contient généralement :
- une date ;
- une source ;
- une facility ;
- une priorité / gravité ;
- un message ;
- parfois l'hôte ou le processus.
- Le démon historique est `syslogd`, mais les systèmes modernes utilisent souvent `rsyslog`, `syslog-ng` ou le journal systemd.

3. `syslog.conf`

> Une règle syslog dit : tels messages vont vers telle destination.

3. `syslog.conf` — Forme générale

```
facility.priority    destination
```

- Exemple conceptuel :

```
authpriv.info        /var/log/auth.log
*.emerg              *
*.*                  @192.168.10.42
```

3. `syslog.conf` — Facilities à expliquer

```
auth/authpriv   authentification et sécurité
user            messages utilisateur
kern            noyau
daemon          démons système
mail            messagerie
local0-local7   usages locaux
```

3. `syslog.conf` — Destinations possibles

```
/var/log/messages      écrire dans un fichier
user2                  notifier un utilisateur
@192.168.10.42         envoyer vers un serveur de logs distant
```

4. Surveillance des logs avec logcheck

> logcheck automatise la lecture régulière des logs et remonte les événements inhabituels.

4. Surveillance des logs avec logcheck

- `logcheck` scrute les logs, généralement toutes les heures, et envoie par mail les messages suspects ou inhabituels.
- Le fichier `/etc/logcheck/logcheck.logfiles` indique les fichiers surveillés.
- Modes de fonctionnement :
- **paranoid** : très verbeux, adapté à des systèmes sensibles comme des pare-feu ;
- **server** : mode recommandé pour serveurs ;
- **workstation** : moins verbeux.

4. Surveillance des logs avec logcheck — Règles logcheck

- Les règles sont réparties selon leur rôle :

```
/etc/logcheck/cracking.d/
/etc/logcheck/cracking.ignore.d/
/etc/logcheck/violations.d/
/etc/logcheck/violations.ignore.d/
```

4. Surveillance des logs avec logcheck — Point d'attention

- Un outil d'alerte mal réglé finit ignoré.
- Il faut réduire le bruit pour que les alertes restent utiles.

5. Vérification d'intégrité avec AIDE

> AIDE compare l'état actuel du système avec une empreinte de référence.

5. Vérification d'intégrité avec AIDE

- AIDE, Advanced Intrusion Detection Environment, crée une base de données à partir de règles.
- Cette base décrit l'état attendu de certains fichiers et répertoires : hash, permissions, propriétaire, groupe, taille, dates, inode, ACL, attributs étendus, contextes SELinux selon configuration.
- Lors d'un contrôle, AIDE compare l'état actuel à l'état de référence et signale les écarts.

5. Vérification d'intégrité avec AIDE

1. Définir ce que l'on surveille.
2. Initialiser la base de référence sur un système sain.
3. Stocker cette base dans un endroit protégé.
4. Exécuter régulièrement un contrôle.
5. Analyser les différences.

5. Vérification d'intégrité avec AIDE — Point d'attention

- AIDE détecte un changement, mais ne décide pas à lui seul si ce changement est légitime ou malveillant.

6. Suivre l'activité mémoire et système

> Avant de redémarrer un serveur lent, il faut savoir quelle ressource manque.

6. Suivre l'activité mémoire et système — free

- Vue rapide de la mémoire :

```
free -h
```

- À expliquer : mémoire utilisée, libre, buffers/cache, swap.

6. Suivre l'activité mémoire et système — vmstat

- Suivi temps réel :

```
vmstat 1
```

- Colonnes importantes à commenter :

```
r   processus en attente CPU
b   processus bloqués en I/O
swpd swap utilisée
free mémoire libre
si/so swap in/out
us/sy/id/wa répartition CPU
```

6. Suivre l'activité mémoire et système — sysstat

- Le paquet `sysstat` fournit notamment :

```
iostat
sar
```

- `iostat` suit surtout les I/O disque.
- `sar` permet de collecter et relire de nombreuses métriques système dans le temps.