Supervision, journaux et rsyslog

Formation : BTS SIO — Option SISR

1. Rôle et fonctionnement

La supervision mesure la disponibilité et les performances, puis déclenche des alertes. La journalisation enregistre les événements. Les deux se complètent : un service peut répondre tout en produisant des erreurs, et un fichier de journal peut exister sans être correctement alimenté.

`journald` collecte les événements systemd ; rsyslog peut les traiter, écrire des fichiers et transmettre des messages à un collecteur. Installer rsyslog ne configure pas automatiquement une centralisation distante.

2. Contrôle local

```
systemctl --failed
sudo journalctl -u unbound -b --no-pager
sudo systemctl status rsyslog
sudo rsyslogd -N1
logger -t recette-labo 'Test de journalisation'
```

`rsyslogd -N1` valide la configuration. Rechercher le message de test dans la destination définie par les règles ; le nom du fichier dépend de la distribution et des réglages.

3. Concevoir la collecte

Définir les équipements émetteurs, le collecteur, le transport, la rétention et les accès. Prévoir la rotation et l'espace disque. Une collecte distante sur un réseau non maîtrisé nécessite une protection appropriée, par exemple TLS, et une authentification du collecteur.

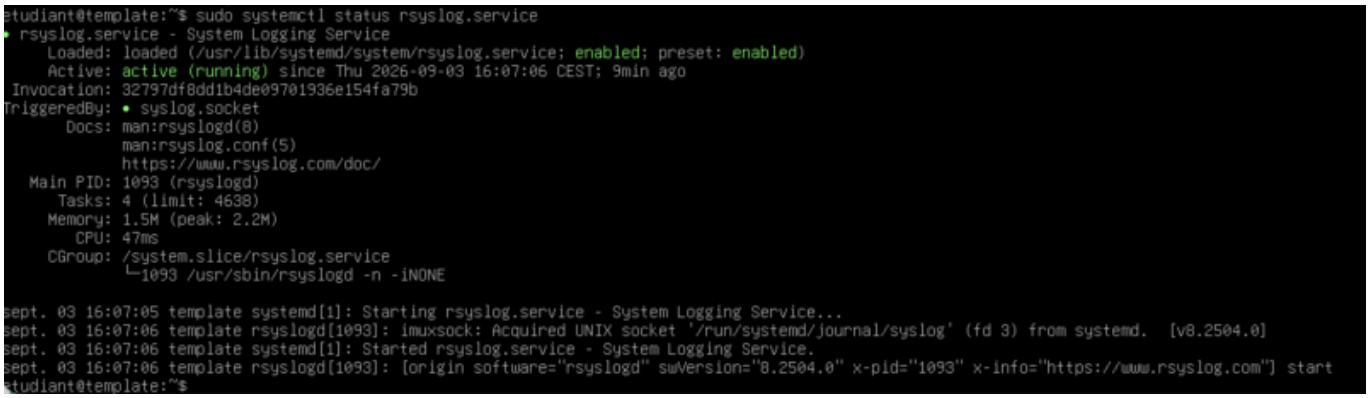
Zabbix ou Nagios peuvent superviser des services, mais leur déploiement complet exige une configuration propre, éventuellement une base de données et un serveur Web. Leur seule installation ne suffit pas à créer une supervision opérationnelle.

4. Recette et dépannage

Contrôle	Attendu
Service arrêté volontairement en maquette	Alerte reçue
Service rétabli	Retour à l'état normal
Message de test	Présent sur le collecteur
Horodatage	Cohérent avec les autres équipements
Rotation	Espace disque maîtrisé

En cas d'absence d'événements, vérifier émission, filtrage, transport, règles du collecteur et permissions de destination. Utiliser une capture ciblée pour localiser la rupture.

5. Contrôles conservés



État du service rsyslog dans le laboratoire.



Fichiers de journaux présents dans /var/log.

Ces captures documentent une journalisation locale. Elles ne démontrent pas une centralisation distante ni un système d'alertes opérationnel.

6. Références

- Debian — rsyslogd
- Debian — tcpdump

From:
https://wiki.ewengadonnaud.xyz/ - **Base de savoir réseaux/cyber/devops**

Permanent link:
https://wiki.ewengadonnaud.xyz/doku.php?id=services:journalisation

Last update: **2026/10/18 01:23**