Déploiement NTP + Syslog

1. NTP - Synchronisation temporelle

Objectif : Garantir une horodatage cohérent sur tous les équipements, indispensable pour corréler les logs.

- Chaque équipement Cisco (switchs + routeur) est configuré en client NTP pointant vers le serveur NTP du projet.
- La commande "ntp server <IP>" est appliquée sur chaque équipement.
- Le service "service timestamps log datetime msec" est ctivé pour horodater les logs avec précision (millisecondes).
- La timezone est uniformisée "clock timezone"

2. Syslog - Centralisation des journaux

Objectif : Collecter les événements réseau de tous les équipements vers un point central pour analyse et archivage.

Sur les équipements Cisco :

- Envoi des logs vers le NAS : "logging host 192.168.99.7"
- Niveau de sévérité retenu : informational (niveau 6)
- Action des événements pertinents :
  - logging buffered (tampon local)
  - archive log config (changements de configuration)
  - Spanning-Tree, authentification (login), interfaces

Sur le serveur de logs (Ubuntu 22.04.5 LTS)

- Rsyslog configuré pour recevoir les logs UDP / TCP (port 514) et les router par équipement dans "/var/log/cisco/<nom-équipement>.log
- Rotation des logs via "logrotate" avec rétention 365 jours (recommandation ANSSI)
- Loganalyzer déployé comme interface web de consultation et d'analyse des logs

3. Limitation du buffer de logs sur les Cisco

Objectif : Eviter la saturation de la mémoire des switchs et routeur.

```
logging buffered 16384 informational
```

- 16384 octets (16Ko) - valeur raisonnable pour un swich/routeur
- Evite la consommation excessive de RAM tout en gardant un historique local court.

```
no logging console     OU     logging console critical
```

Le logging console est très gourmand si une session est active. Le couper ou ne garder que les événements critiques est une bonne pratique.

```
no logging monitor
```

Inutile en production / démo, consomme des ressources inutilement.

```
logging host 192.168.99.7
logging trap informational
```

Le NAS stocke, le switch transmet et puis oublie.

Revision #1
Created 21 May 2026 06:22:42 by Raphaël
Updated 21 May 2026 06:41:28 by Raphaël