Mission 3 — Paramétrer les logs sur routeurs & switchs

Objectif : Envoyer les journaux vers un serveur central (rsyslog) tout en gardant un buffer local.
--> A le faire a chaque équipement

Sur PuTTy, sur le routeur :

1.1. Activer l'horodatage (obligatoire pour CNIL/RGPD) :

```
conf t
service timestamps log datetime msec localtime show-timezone
service sequence-numbers
```

1.2. Envoyer les logs au serveur Syslog

```
logging host 192.168.99.3
logging trap informational
logging on
```

1.3. Inclure les informations critiques

Logs des tentatives administratives (SSH, console, login)

```
login on-failure log
login on-success log
ip ssh logging events
```

Logs des changements de configuration

```
archive
log config
  logging enable
  notify syslog
  hidekeys
```

1.4. Suivi des interfaces (up/down + erreurs)

```
conf t
   logging event link-status
   logging event trunk-status
```

Pour une interface spécifique :

```
interface GigabitEthernet0/1
   logging event link-status
```

1.5. Logs ACL (accés refusés)

Ajoute log à la fin des ACL :

```
ip access-list extended SECURITE
deny ip any any log
permit ip any any
```

1.6. Logs sécurité L2 (si switch - routeur hybride)

Sur routeurs L3 avec switch intégré :

```
ip dhcp snooping database write-delay 60
ip arp inspection logging
```

1.7. Logs NTP

```
ntp logging
```

1.8. Logs système

```
logging buffered 16384 warnings
```

Sur PuTTy, sur le swicth :

2.1. Activer horodatage

```
service timestamps log datetime msec localtime show-timezone
service sequence-numbers
```

2.2. Envoi vers serveur Syslog

```
logging host 192.168.99.10
logging trap informational
logging on
```

2.3. Port - Security (violation des MAC)

```

```

2.4. DHCP Snooping (serveur DHCP protégé)

Activation globalement :

```
ip dhcp snooping
ip dhcp snooping vlan 10,20,30,40,50
```

Marquer les ports trusted (vers serveur DHCP ou routeur) :

```
interface GigabitEthernet0/1
ip dhcp snooping trust
```

Logs spécifiques :

```
ip dhcp snooping information option allow-untrusted
```

2.6. Spanning Tree (STP)

```
spanning-tree logging
```

2.7. Interface up/down :

Pour forcer logs :

```
interface range Fa0/1 - 48
  logging event link-status
```

Revision #4
Created 15 March 2026 19:51:58 by Raphaël
Updated 2 April 2026 08:17:59 by Raphaël