Mettre en place un service permettant de recueillir ces logs et de pouvoir les consulter (serveur de logs)

Serveur de logs

Infrastructure mise en place

Composant	Détail
Serveur	VM ubuntu test ProXmox
IP	192.168.99.7
OS	Ubuntu 22.04.5 LTS
Service de collecte	rsyslog 8.2112.0
Interface web	Loganalyzer 4.1.13
Port d'écoute	UDP 514

---

1. Installation rsyslog

```
sudo apt update && sudo apt install rsyslog -y
sudo systemctl enable rsyslog
sudo systemctl start rsyslog
```

2. Activation réception UDP 514

Dans `/etc/rsyslog.conf`, décommenter :

```
module(load="imudp")
input(type="imudp" port="514")
```

3. Configuration du tri par équipement

`/etc/rsyslog.d/cisco.conf` :

```
:fromhost-ip, isequal, "192.168.99.14" /var/log/cisco/switch_bat_a.log
& /var/log/cisco/all.log
& stop

:fromhost-ip, isequal, "192.168.99.13" /var/log/cisco/switch_bat_b.log
& /var/log/cisco/all.log
& stop

:fromhost-ip, isequal, "192.168.99.1" /var/log/cisco/routeur.log
& /var/log/cisco/all.log
& stop
```

4. Création du dossier et droits

```
sudo mkdir -p /var/log/cisco
sudo chown syslog:adm /var/log/cisco
sudo chmod 755 /var/log/cisco
sudo chmod 644 /var/log/cisco/*.log
sudo systemctl restart rsyslog
```

5. Rotation des logs (365 jours)

`/etc/logrotate.d/cisco` :

```
/var/log/cisco/*.log {
    daily
    rotate 365
    compress
    missingok
    notifempty
    postrotate
        systemctl restart rsyslog
```

```
    endscript
}
```

6. Installation Loganalyzer

```
sudo apt install apache2 php libapache2-mod-php -y
cd /tmp
wget https://download.adiscon.com/loganalyzer/loganalyzer-4.1.13.tar.gz
tar xzvf loganalyzer-4.1.13.tar.gz
sudo cp -r loganalyzer-4.1.13/src /var/www/html/loganalyzer
sudo chmod 777 /var/www/html/loganalyzer
cd /var/www/html/loganalyzer
sudo touch config.php
sudo chmod 666 config.php
```

7. Droits de lecture Loganalyzer

```
sudo chmod 644 /var/log/syslog
sudo chmod 644 /var/log/cisco/*.log
```

8. Vérifications

```
# Port 514 ouvert
sudo ss -ulnp | grep 514

# Paquets reçus
sudo tcpdump -i any port 514 -nn

# Fichiers de logs
ls /var/log/cisco/

# Logs en temps réel
tail -f /var/log/cisco/switch_bat_a.log
tail -f /var/log/cisco/switch_bat_b.log
tail -f /var/log/cisco/routeur.log

# Validation config rsyslog
sudo rsyslogd -N1 2>&1
```

Résultat final

- Logs reçus en temps réel depuis les 3 équipements
- Fichiers séparés par équipement
- Rotation 365 jours
- Interface web Loganalyzer accessible sur `http://192.168.99.7/loganalyzer`
- Filtrage par Facility, Severity, Hostname disponible

Revision #2
Created 11 May 2026 07:29:35 by Raphaël
Updated 14 May 2026 14:44:27 by Raphaël