Voici une procédure courte, propre et prête à partager — en anglais comme demandé (avec une traduction FR sous l'original).

SIEM Log Collection Performance — Quick Diagnostic Procedure

Account & host

- SSH into the target node using the `li-admin` account.

Working directory

```
cd /opt/makalu/var/log/benchmarker
```

1) Ingestion (Syslog Collector)

Follow live ingestion to spot drops, throttling, or backlogs.

```
tail -F -n 0 syslog_collector.log
```

2) Normalization

Track the four normalization threads plus the front queue/dispatcher.

```
# 4 normalization threads
tail -F -n 0 normalizer_?.log
# front stage
tail -F -n 0 norm_front.log
```

3) Indexing (per repository)

Check indexing latency and commit cycles per repo.

```
# Replace <repo name> with the actual repository identifier
tail -F -n 0 indexsearcher_<repo name>.log
```

4) Journaling / Storage

Verify write throughput and any persistence slowdowns.

```
tail -F -n 0 store_handler.log
```

5) Process-level Metrics (optional, for quick triage)

> Run these in another terminal while logs are streaming.

```
# Top CPU/memory consumers
ps -eo pid,comm,%cpu,%mem --sort=-%cpu | head

# Per-thread view for target processes (if permitted)
top -H -p $(pgrep -d, -f 'syslog_collector')
top -H -p $(pgrep -d, -f 'normalizer')
top -H -p $(pgrep -d, -f 'indexsearcher')
top -H -p $(pgrep -d, -f 'store_handler')

# Disk & memory snapshots (if available)
iostat -xz 1 5    # requires sysstat
free -m
df -h
```