🔍 Full Buffer Debug Procedure (ESA relay, RFC 5424 + Fake Host)

1) Prerequisites

- Relay config:

  ```
  queue.type="LinkedList"
  queue.filename="q_logpoint_tls"
  queue.maxdiskspace="10g"
  ```

- Inputs enabled:
  - `imudp` on port 514
  - `imtcp` on port 514
  - `imtcp` with TLS on port 6514

- `impstats` enabled and writing to `/var/log/rsyslog_stats.json`.

- **Important**: In the SIEM backends, configure a device named **`mytesthost`** so that messages from this fake host are accepted and visible.

- Verify `logger` supports `--host` and `--rfc5424`:

  ```
  logger --help | egrep 'rfc5424|host'
  ```

---

2) Generate baseline traffic

Context: Confirm that normal forwarding works and SIEM accepts the fake host.

Send 10 test messages in **RFC 5424** format with hostname `mytesthost` via TCP/514:

```
for i in {1..10}; do \
  logger --rfc5424 --host="mytesthost" -t BUFFER_TEST --tcp -n 127.0.0.1 -P 514 "baseline msg $i"; \
done
```

👉 In the SIEM GUI, you should see events from device **mytesthost**, tag **BUFFER_TEST**, messages `baseline msg 1…10`.

---

3) Simulate outage (block all targets)

Option A — iptables

```
sudo iptables -I OUTPUT -p tcp --dport 6514 -j DROP
```

Remove:

```
sudo iptables -D OUTPUT -p tcp --dport 6514 -j DROP
```

Option B — firewalld

```
sudo firewall-cmd --add-rich-rule='rule family="ipv4" port port="6514"
protocol="tcp" reject' --timeout=300
```

Remove:

```
sudo firewall-cmd --remove-rich-rule='rule family="ipv4" port port="6514"
protocol="tcp" reject'
```

---

4) Confirm suspension

Context: Rsyslog action must suspend when all targets unreachable.

```
grep -i 'omfwd.*suspend' /var/log/messages | tail -n5
```

Expected line:

```
omfwd: action 'lp_tls_rr' suspended
```

---

5) Generate test traffic during outage

Context: These should be buffered (memory → disk).

Send 500 RFC 5424 messages with fake host:

```
for i in {1..500}; do \
  logger --rfc5424 --host="mytesthost" -t BUFFER_TEST --tcp -n 127.0.0.1 -P 514
  "msg during outage $i"; \
done
```

---

6) Observe impstats

Context: Queue must be filling.

```
tail -f /var/log/rsyslog_stats.json | grep '"lp_tls_rr"'
```

Look for:

- `suspended=true`
- `queuesize` increasing steadily

---

7) Verify spool files

Context: Disk-assisted queue must persist backlog.

```
ls -lh /var/spool/rsyslog/
du -sh /var/spool/rsyslog/
```

Files `q_logpoint_tls*` should appear and grow.

---

8) Restore targets

- With iptables:

  ```
  sudo iptables -D OUTPUT -p tcp --dport 6514 -j DROP
  ```

- With firewalld:

  ```
  sudo firewall-cmd --remove-rich-rule='rule family="ipv4" port port="6514"
  protocol="tcp" reject'
  ```

---

9) Confirm replay

Context: After recovery, backlog must drain automatically.

Check:

```
tail -f /var/log/rsyslog_stats.json | grep '"lp_tls_rr"'
ls -lh /var/spool/rsyslog/
```

Expected:

- `suspended=false`
- `queuesize` decreases → 0
- spool files shrink/disappear

---

10) Validate in SIEM GUI

Context: All `BUFFER_TEST` events from `mytesthost` (baseline + outage) must appear.

- May be delayed, but **no permanent gap** should remain.

---

11) Optional fallback file

Context: If configured, fallback grows only during suspension.

```
tail -n20 /var/log/esa_fallback-buffer.log
```

Should contain your `BUFFER_TEST` messages if action suspended.

☑ Expected Results

- Outage → `suspended=true`, `queuesize` grows, spool files grow
- Recovery → `suspended=false`, `queuesize` drains, spool shrinks, SIEM shows replay
- All messages visible under device **mytesthost**