

● On-call now Platform rotation, Techsy

● Paging PagerDuty "kestrel-platform", 24/7

● Chat #kestrel-incidents

● Last drill 24 Sep 2026, passed

● Next drill 29 Oct 2026

● Owner Techsy delivery lead

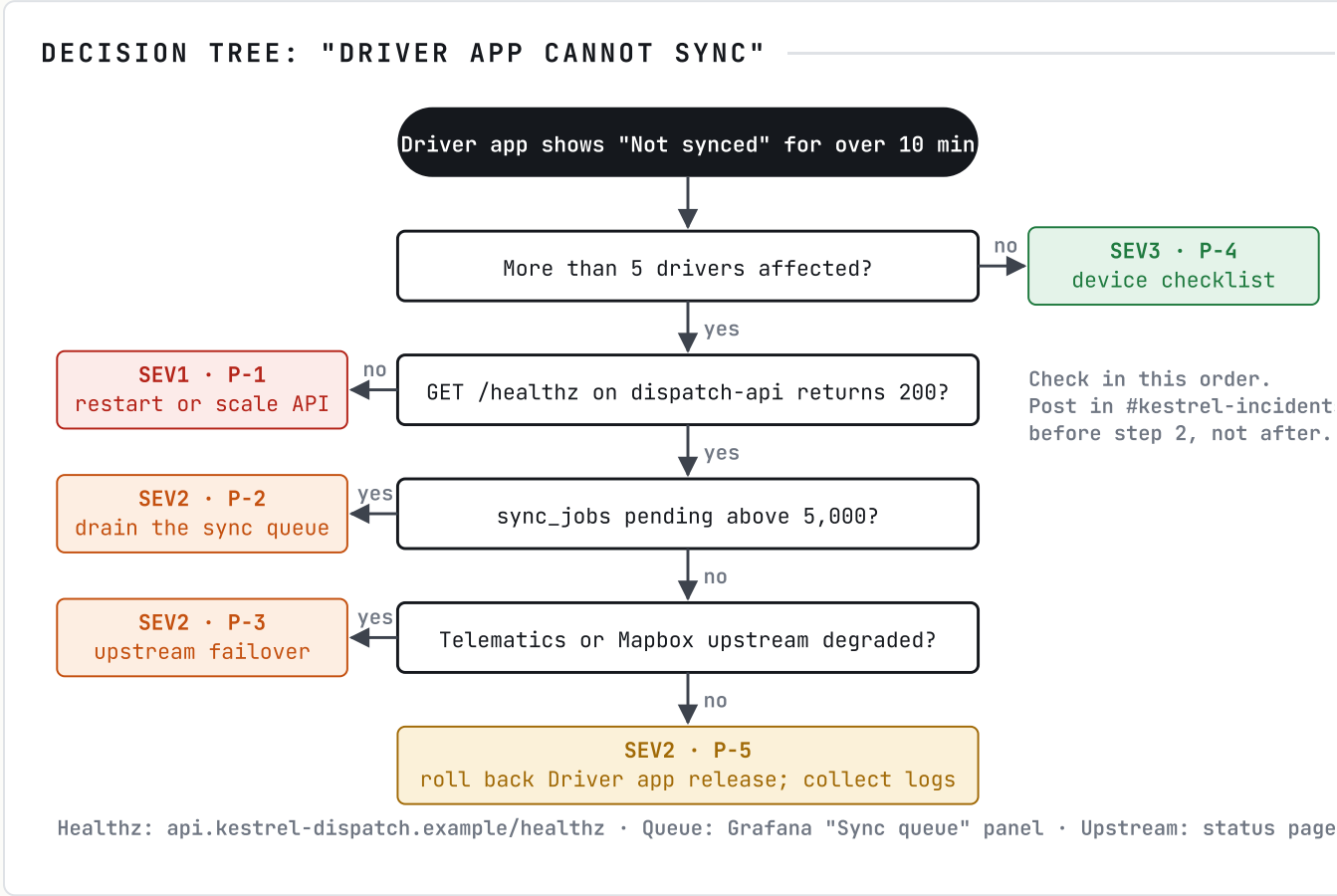
RUNBOOK · INCIDENT RESPONSE · DISPATCH WEB, DRIVER APP, AI ASSISTANT

Runbook: Kestrel Dispatch on-call playbook

What to do in the first 15 minutes when something breaks for Kestrel's dispatchers or drivers. Severity first, then the decision tree, then the numbered procedure. Every step has been run in a drill; if one is wrong, fix the runbook in the same pull request as the fix.

SEVERITY LEVELS

LEVEL	DEFINITION	EXAMPLES	RESPOND WITHIN	UPDATES	WHO IS PAGED
SEV1	Dispatch stopped for a depot or the whole fleet, or data at risk.	Dispatch web down; Driver app cannot sync for more than 5 drivers; Postgres primary lost; wrong plans sent to drivers.	15 min, 24/7	every 30 min	On-call engineer, Techsy delivery lead, Kestrel ops manager
SEV2	One feature or one depot degraded; dispatch continues with a workaround.	ETA pushes late; assistant drafts failing; POD upload slow; shipper portal read-only.	30 min, 06:00-23:00	hourly	On-call engineer; Kestrel depot lead if one depot
SEV3	Cosmetic or single-user; no effect on loads.	One device not syncing; a report off by a day; translation missing in the German portal.	next business day	in the ticket	Nobody paged; ticket to the Techsy board



ESCALATION BY ROLE

ROLE	REACH	WHEN
Techsy on-call engineer rotation in PagerDuty	Page "kestrel-platform"	First, always
Techsy delivery lead Anna	PagerDuty level 2, phone	SEV1 not acknowledged in 15 min, or any SEV1 over 1 h
Kestrel ops manager, Venlo Ruud	Phone, "Kestrel ops" WhatsApp group	All SEV1; SEV2 touching Venlo
Kestrel IT contact, Duisburg Lena	Phone, Teams	SEV1; SEV2 touching Duisburg; anything with SSO
Hosting support Hetzner Cloud	Ticket; phone on the enterprise line	Infra outage confirmed on their status page
Telematics vendor desk 08:00-18:00 CET	Ticket, support phone	P-3 only

Phone numbers live in the PagerDuty contact card and the 1Password vault "Kestrel on-call", never in this file.

P-1 Dispatch API unhealthy

When: /healthz is not 200 or dispatch web shows "Reconnecting". Target: healthy in 10 min.

- 1 Confirm from outside the cluster, then declare SEV1 in #kestrel-incidents.

```
$ curl -s -o /dev/null -w "%{http_code}\n" api.kestrel-dispatch.example/healthz
503
```

- 2 Look at the pods: CrashLoopBackOff points to the database, Pending to capacity.

```
$ kubectl -n kestrel get pods -l app=dispatch-api
dispatch-api-7c9f-k2xq 0/1 CrashLoopBackOff 6 9m
```

- 3 Check the database before restarting anything.

```
$ psql "$DATABASE_URL" -c "select now(), pg_is_in_recovery();"
```

- 4 Restart and wait for the rollout. Scale to 4 if the first restart does not hold.

```
$ kubectl -n kestrel rollout restart deploy/dispatch-api
$ kubectl -n kestrel rollout status deploy/dispatch-api
```

- 5 Post the status page update, then every 30 min until closed.

```
$ ./scripts/status post --sev 1 --msg "Dispatch API degraded"
```

P-2 Drain the sync queue

When: API healthy, sync_jobs pending above 5,000. Target: below 500 in 20 min.

- 1 Measure the backlog and error share; over 10% errors means stop, go to P-5.

```
$ psql "$DATABASE_URL" -c "select status, count(*) from sync_jobs group by 1;"
pending | 12840   done | 418221   failed | 96
```

- 2 Scale the workers from 2 to 6. Each worker clears about 40 jobs per second.

```
$ kubectl -n kestrel scale deploy/sync-worker --replicas=6
```

- 3 Watch the errors; a rising count means the jobs are bad, not slow.

```
$ kubectl -n kestrel logs deploy/sync-worker --since=10m | grep -c ERR
```

- 4 Tell dispatch the ETA (12,840 jobs at 240/s is about a minute). Scale back to 2 when pending is under 500.

```
$ kubectl -n kestrel scale deploy/sync-worker --replicas=2
```

LAST DRILL

24 Sep 2026

Scenario: Postgres primary failover during the 17:00 dispatch peak

RESULT

- Time to recovery **11 min**, target 15 min. Passed.
- Replica promoted at 17:08; API reconnected without a restart.
- Status page posted at 17:04, German version at 17:09.

FINDINGS, FIXED IN REV 9

- P-1 step 3 used the old database hostname. Corrected.
- No German status template existed. Added.
- Next drill 29 Oct: "Driver app cannot sync, Duisburg", run on the Driver 2.0 beta.