**Document: 11 – Monitoring & Observability**

**Project:** MCPX-KendoBridge Admin Portal  
**Document ID:** TJ-MCPX-DOC-11  
**Version:** 1.1.0  
**Status:** Draft  
**Date:** 2025-09-27  
**Owner:** SRE / DevSecOps Lead (Technijian)  
**Confidentiality:** Technijian Internal

**Document Control**

| **Version** | **Date** | **Author** | **Change Summary** | **Status** |
| --- | --- | --- | --- | --- |
| 1.0.0 | 2025-09-26 | Doc-Factory | Initial observability outline | Draft |
| 1.1.0 | 2025-09-27 | DevSecOps | Added SSE **TTFB/heartbeat** monitors, p50/p95/p99 latency, **RTM↔Prod parity** widget & alerts; requestId logging schema | Draft |

**Approvals**

| **Role/Team** | **Name** | **Signature/Date** | **Comment** |
| --- | --- | --- | --- |
| Director of Software Eng. |  |  |  |
| Systems Architect |  |  |  |
| Security/Compliance |  |  |  |
| QA Lead |  |  |  |

**1. Purpose**

Define **what we measure, visualize, and alert on** so the Admin Portal meets its SLOs, with clear **runbooks** and **evidence** captured for each release.

**2. Scope**

* **Admin API (.NET 8)** and **Web (React + KendoReact Fluent 2)**
* **SSE channels** (jobs & notifications)
* **SQL Server 2022** (SP-only DAL)
* **Azure SSO** success/error rates (via app metrics & logs)
* **RTM↔Prod configuration parity** status

**3. References**

* 04 System Context, 05 NFRs, 09 Test Strategy, 10 CI/CD, 12 Evidence Pack, 16 DoR/DoD, Runbooks (/runbooks/\*.docx)

**4. Telemetry Standards**

**4.1 Correlation**

* **requestId**: generated at ingress; **must** propagate across Web→API→Jobs.
* **jobId**: for long-running tasks; included in SSE events and completion logs.
* **Trace context** (if tracing enabled): traceId/spanId attached to logs and metrics labels.

**4.2 Log Schema (JSON lines)**

Minimum fields:

timestamp, level, requestId, userId?, role?, route, method, status, latency\_ms,

sse: { connection\_id?, first\_event\_ms?, heartbeat\_gap\_ms? },

job: { jobId?, state? },

error: { code?, message? }, env, version, server

* **Never** log secrets or PHI.
* Errors use the **standard envelope** codes (see Error Catalog).

**4.3 Metric Labeling**

* Common labels: env, service, route, status, role, version, instance.
* Cardinality guardrails: avoid high-cardinality labels (e.g., raw requestId).

**5. Service Level Indicators (SLIs) & SLOs**

(From NFRs; measured monthly unless noted.)

| **Area / Metric** | **Definition** | **SLO (Prod)** |
| --- | --- | --- |
| API availability | Uptime minutes / total minutes | **≥ 99.9%** |
| Web availability | SPA served + API reachable (synthetic login+dashboard) | **≥ 99.9%** |
| JSON read latency | p95/p99 for GET endpoints | **p95 ≤ 300 ms**, **p99 ≤ 600 ms** |
| JSON write latency | p95/p99 for mutations | **p95 ≤ 500 ms**, **p99 ≤ 900 ms** |
| /healthz latency | p95 | **≤ 150 ms** |
| **SSE TTFB** | First event time (ms) | **≤ 200 ms** |
| **SSE heartbeat cadence** | Max gap between heartbeats | **≤ 10 s** |
| Dashboard TTI | Time to interactive after auth | **p95 ≤ 2.0 s** |
| 5xx error rate | 5xx / total | **≤ 0.5%** |
| RTM↔Prod **parity** (critical) | Critical diffs count | **= 0** before Prod |

**6. Metrics Catalog (names are exemplary; adapt to your stack)**

**API HTTP**

* api\_requests\_total{route,method,status}
* api\_request\_duration\_ms\_bucket{route,method} (histogram → p50/p95/p99)
* api\_errors\_total{code} (envelope code)

**SSE**

* sse\_connections\_open{route}
* sse\_first\_event\_ms{route} (summary)
* sse\_heartbeat\_gap\_ms{route} (gauge; last observed gap)
* sse\_reconnects\_total{route,reason}

**Jobs**

* job\_started\_total{type}
* job\_duration\_ms\_bucket{type}
* job\_failed\_total{type,code}

**Auth / Security**

* auth\_success\_total, auth\_failure\_total{reason}
* cors\_denied\_total{origin}
* rate\_limited\_total{route}

**DB (SP-only)**

* db\_sp\_duration\_ms\_bucket{name}
* db\_sp\_errors\_total{name,code}

**Parity / Readiness**

* parity\_critical\_diffs{env} (gauge)
* ready\_status{env} (0/1)

**Web**

* web\_tti\_ms (p95), web\_bundle\_kb (gauge for first route)

**7. Dashboards (by environment)**

**7.1 Executive (Landing)**

* Availability (API/Web)
* Error rate, p95 latency (global)
* **Parity status** (RTM: Ready/Blocked + #critical diffs)
* Release version & commit SHA

**7.2 API Performance**

* Requests by route & status
* p50/p95/p99 latency histograms
* Top error envelope codes
* DB SP latency top-N

**7.3 SSE Health**

* Connections open & reconnect rate
* **First-event (TTFB) trend** (target ≤ 200 ms)
* **Heartbeat gap** (max, avg) with threshold line at 10 s
* Per-job SSE duration & failures

**7.4 Jobs & Queues**

* Jobs started/completed/failed by type
* Duration distributions; slowest recent jobs
* Failures by error code

**7.5 Security**

* Auth failures (by reason)
* CORS denies (by origin)
* Rate-limited requests (by route)

**7.6 Readiness & Parity**

* /healthz p95, component statuses
* /ready timeline (1/0)
* **Parity diff count** (critical/major/minor), with link to full report

**8. Alerts & Policies**

Alerting should be **actionable**, **deduplicated**, and linked to a runbook step.

| **Alert** | **Condition (Prod)** | **Duration** | **Action / Runbook** |
| --- | --- | --- | --- |
| API availability drop | < 99.9% over last 1h | 5m | Check deploy health; rollback if needed |
| 5xx error spike | > 1% for 5 min | 5m | Inspect latest deploy; error codes; throttle callers |
| p95 JSON latency breach | > 600 ms for 10 min | 10m | DB/SP hot path review; scale out; cache |
| **SSE TTFB breach** | median > 200 ms for 10 min | 10m | Investigate child process/backpressure |
| **SSE heartbeat gap** | gap > 15 s (single instance) | 1m | Check worker health; network; restart child |
| CORS denied anomaly | 10+ denies/min for 5 min | 5m | Validate allow-list; suspicious origin |
| Rate-limiting surge | 100+ 429/min | 5m | Abuse or bug; inspect client IDs |
| Readiness flapping | /ready toggles > 3 times in 10 min | 10m | Dependency instability; hold deploy |
| **Parity gate blocked** (RTM) | critical\_diffs > 0 | instant | Block promotion; open remediation task |

**Severity mapping:**

* **P1**: Availability, readiness flapping, parity blocked during release.
* **P2**: SSE heartbeat/TTFB, 5xx spikes, p95 breach.
* **P3**: CORS/rate-limit anomalies.

**9. Synthetics & Smoke**

* **Login & Dashboard**: headless browser signs in (MSAL), lands on /dashboard, verifies env badge, cards render.
* **Config Read**: GET /config/effective 200 with non-secrets only.
* **SSE Smoke**: k6 script exercises /jobs/{id}/events and validates **TTFB ≤ 200 ms** and **heartbeat ≤ 10 s**.
* **Parity Probe (RTM)**: scheduled parity check; publish delta counts to parity\_critical\_diffs.

**10. Evidence & Retention**

For each **release** (per 12\_evidence\_pack):

* Export **dashboard screenshots** (Executive, SSE Health, Parity)
* Include **alert policy export** (JSON/YAML)
* Attach **k6 results** & **parity report**
* Retain **≥ 1 year** with the tag

**11. Runbooks (hooks)**

* **Deploy / Rollback**: update “current version” annotation; confirm /ready green and parity 0 critical.
* **Incident**: triage checklist (logs → metrics → recent deploy/flags → rollback) with **requestId** drill-through.
* **Scale Out**: verify p95 improvements and SSE first-event after scaling.

(See /runbooks/deploy.docx, rollback.docx, incident.docx, scale\_out.docx.)

**12. Implementation Tasks**

1. Instrument API with **request/response** histograms & envelope code counters.
2. Emit **SSE metrics** (first-event ms, heartbeat gap, reconnects).
3. Add **parity exporter** (RTM) to expose parity\_critical\_diffs.
4. Wire **synthetics** (login→dashboard) and **k6** job into nightly CI.
5. Create **Grafana (or equivalent)** dashboards per §7; export JSON in repo.
6. Commit **alert policies** (YAML/JSON) under /monitoring/alerts/ and reference in runbooks.
7. Add **release-time screenshot** job for Evidence Pack.

**13. Acceptance Criteria**

* Dashboards exist for **Executive**, **API Performance**, **SSE Health**, **Security**, **Readiness & Parity**.
* Alerts configured per §8 and route to the correct on-call.
* **SSE TTFB** and **heartbeat** metrics visible and tracked against thresholds.
* **Parity widget** shows **Ready/Blocked** and counts of critical/major/minor diffs in RTM.
* Synthetics and k6 smoke run nightly; results attached to releases.
* Evidence Pack includes dashboard screenshots, alert policy export, k6 results, and parity report.

**14. Open Issues**

* Finalize metric backend (e.g., Azure Monitor/Grafana/ELK) naming conventions.
* Decide whether to expose public status (likely **no**; internal only).
* Confirm which parity keys are **critical** vs **minor** (owning team + Security).

**End of Document — TJ-MCPX-DOC-11 v1.1.0**