Sibuna Discussions SID 0007

The Sibuna Console: A Real-Time Management Interface for Nodes and Clusters in Pure Zig

STATE
committed
STATUS
Committed
TYPE
Architectural Specification
AUTHORS
Sibuna Contributors <team@sibuna.local>
CREATED
2026-09-08
UPDATED
2026-10-15

SUMMARY

Specifies the Sibuna Console, a complete management interface for Sibuna: a separate pure-Zig module started from the Sibuna CLI that serves a real-time web interface over the standard library's HTTP server and WebSockets, renders its pages from a WebAssembly module styled with daisyUI 5, keeps authentication, statistics, audit, and a GeoIP database in the embedded Zaxonlite store, manages one node or a replicated cluster, and defines performance acceptance targets that remain to be measured.

DISCUSSION

No external discussion URL assigned

LABELS

console, management, websocket, ui, zaxonlite, geoip, cluster

Record status

The catalog defines the review process and the meaning of each state. This numbered record forms part of the catalog.

Contents

1. Revision note 2
2. Abstract 7
3. Introduction and Motivation 8
4. Operator Workflows 8
5. Design Principles 9
6. Terminology and Scope 12
7. Goals and Non-Goals 12
8. Architecture Overview 13
9. The Serve Kernel 16
10. Authentication and Authorization 17
11. The Telemetry Pipeline 18
12. The Real-Time Protocol 20
13. Data Model 22
14. GeoIP 23
15. Cluster Management 25
16. The Interface Module 25

17. Wireframes 27
18. The Build Pipeline 37
19. Security Considerations 38
20. Performance Budget 38
21. Delivery Plan 39
22. Verification 40
23. Resolved Design Decisions 40
24. Operational Contracts and Trade-offs 41
25. Acceptance and Open Questions 43
26. References 45

1. Revision note

2026-10-15: Ported from the Typst original in the Zig repository. The record describes the Zig implementation as it was decided; SID 0010 maps its packages to the Rust crates of the port. In the Rust port the console server and its WebAssembly interface are Rust crates, and storage uses sqlx (SID 0011) instead of Zaxonlite; SQLite triggers described here become explicit transactional statements so both SQLite and PostgreSQL enforce the same invariants.

2026-10-15 (Rust port, listener admission): the accepted deviation that left `admission.zig` an unwired reference no longer holds. The Rust listener (`sibuna-serve`) admits every connection in the HTTP class and moves an upgraded connection to the browser or peer class in one step, with the same bounds (96 slots, 16 reserved for HTTP, at most 64 browser and 16 peer streams). The 65th browser subscriber is refused by admission, and the console still answers it with its own 503. Outbound connections from the console use TLS through rustls (SID 0012).

2026-10-15 (Rust port, rankings archives): the Zig console bounded an SBR2 archive at 48,528 bytes because it counted the referrer section header as 4 bytes instead of 12. The largest SBR2 archive (256 path counters and 256 referrer counters) is 48,536 bytes, so a minute with both sketches full was refused and never archived, contrary to this record's requirement that the archive retain every counter. The Rust console bounds archives at 48,536 bytes and stores such minutes; archives Zig wrote are unaffected.

2026-10-15 (Rust port, service kernel): `sibuna-serve` parses heads with `sibuna_http::parse_request` instead of `std.http.Server.receiveHead`. Its grammar is stricter (whitespace before a colon, more than 32 fields and conflicting framing are refused), and the refusal is the same as before: the connection closes without a reply. Zig's other refusals are kept. A body cut short by the peer is an error, where Zig's reader returned the short body as complete. Deadlines are kept in milliseconds, so a 10-second deadline lasts 10 seconds rather than 9 to 10. The extra header fields of a response are no longer limited to four. Service threads reserve their usable 256 KiB without the additional 256 KiB signal stack of Invariant I4: the Rust standard library maps its signal stack separately and never requests less than glibc's minimum stack, which accounts for static TLS. The acceptor sleeps 10 ms after a failed `accept` instead of retrying at once. The bytes of every response (status lines and reason phrases, the 503, 431, 100 Continue and 101 heads, the security fields) are unchanged.

2026-10-15 (Rust port, rendering): `sibuna-html` compiles the snippets in a build script into Rust functions, each with a generated values struct, instead of expanding them with comptime. The accepted syntax, the checks and their order, and the rendered bytes are unchanged; golden tests compare all 80 console snippets with the output of the Zig renderer. Four differences follow from the move to Rust: a missing value is a compile error at the call site rather than `HTML004` (which remains for rendering by name), a placeholder that Rust cannot name as a field fails with `HTML006`, the new code `HTML008` requires a snippet file name that yields Rust item names, and text values must be valid UTF-8. A call passes exactly the snippet's fields, where Zig ignored extra values. The dictionary packing of literal text and the compact template interpreter, which existed to shrink the WebAssembly module, are not ported: literal runs are string constants. Their effect on the interface module budget is to be measured when the module is ported.

2026-10-15 (Rust port, interface module): the Zig module rendered each page into a fixed 512 KB output buffer, wrote its commands into a fixed 16 KiB buffer, parsed each event in a fixed 512 KiB bump arena and ran in a fixed 4 MiB linear memory, because Zig had no allocator in `wasm32-freestanding`. The Rust module (`sibuna-console-ui` for `wasm32-unknown-unknown`) uses owned, reused strings and the parsed event tree instead. The bounds that protect the browser stay explicit: an event is at most the largest retained rankings reply plus its envelope, a rendered page at most 512 KiB (a page that exceeds it is not shown, as before),

JSON nesting at most 64 levels, the geometry at most 128 KiB, and linear memory grows on demand up to a declared maximum of 16 MiB (the largest event's parse tree peaks near 3.6 MiB). The command list has no bound of its own, because it is a function of the bounded event and the bounded state; Zig failed an action whose commands exceeded 16 KiB. The secure erasure of the event arena became an allocator that zeroes every block it frees, together with explicit wiping of the reused input, page and command buffers. The bridge (`glue.js`), the module's exports and the event and command formats are unchanged, and the golden fixtures are byte-identical. Pages are independent modules behind one interface. The budget (768 KiB ceiling, 640 KiB review threshold) is unchanged; the core with its first page measures 271,005 bytes.

2026-10-15 (Rust port, GeoIP and passwords): `sibuna-geoip` accepts the same CSV rows and reports the file and line of a refused row. Its `SBGEOIP1` decoder also requires the bytes after the version text and the unused file-digest slot of a one-file provider to be zero. The Zig encoder always wrote zeros, so every snapshot it wrote still decodes, and each snapshot now has exactly one encoding. A loader reserves no capacity up front (Zig reserved space for 1,048,576 ranges), so the memory of a generation follows its row count: 34 bytes per range in three sorted arrays. Gzip archives are decompressed by `sibuna-inflate`, which also checks the header CRC when the FHCRC flag is set and rejects reserved flag bits, as RFC 1952 requires; Zig skipped both. A second gzip member, a CRC or size mismatch and trailing bytes are still refused as one checksum error. Argon2id (`sibuna-crypto`) runs over a caller-owned workspace of 1 KiB blocks, which is wiped before it returns, instead of an allocator over the reserved buffer, and runs lanes in sequence; the console uses one lane, so hashes are unchanged. PHC verification checks the costs against the configured maxima before it touches memory and compares hashes in constant time. A parameter list containing `alg_version=`, which made Zig's parser panic, is refused as an invalid encoding.

2026-10-15 (Rust port, globe): the Zig globe wrote the two bytes of a country code raw into the `<title>` of a country marker and of a connection, while every other value of the console is escaped. Country codes come from the statistics snapshot, whose decoder accepts any 16-bit code, so a code such as `<!` would have reached the SVG as markup. The Rust globe escapes these titles like every other value; for the two capital letters of a real country code the markup is unchanged, so no fixture changes. The animation keeps its turned view in the globe module and writes it back into the shared view at the next event, because a frame borrows the shared state read-only; frames are byte-identical to the Zig module's.

2026-10-15 (Rust port, management pages): the users, tokens, audit, settings (with the response-page editor), nodes and GeoIP pages are ported. Their replies decode with the console protocol's types, which refuse members they do not know where the Zig wire structs ignored them. Three changes follow from reviews and bugs. First, SID 0013 drops the Zaxonlite log frontiers `applied_slot` and `decided_slot` from the node row, because the Rust port has no consensus log; the member card no longer shows the rows "Log slots: applied / decided" and "Replication lag" derived from them, and shows the member's applied policy revision against the committed revision instead, as it already did. The `nodes` fixture is unchanged, because its membership is not loaded; a test covers the card. Second, the Zig settings page set "Saved." after a saved destination, removal or setting change and then cleared it at once with the refresh it sent, so the operator never saw it; the Rust page sets the message after the refresh. Third, the About facts are read when they arrive instead of being kept as JSON text in a 512-byte buffer that refused a longer reply.

2026-10-15 (Rust port, recovery codes): the Zig interface cleared the CSRF token as soon as `totp-confirm` succeeded, because enabling two-factor authentication ends the session. The renderer then drew the sign-in card for the `security` phase, and the ten recovery codes, which the server returns only once, were never displayed. The Rust page keeps the two-factor page on screen while the codes are pending: the session is held in the restricted state of a required enrollment (no navigation shell, no live connection, no other page or request), and every action except the acknowledgement and the appearance toggles is refused. The acknowledgement erases the codes, drops the token and opens the sign-in page, as Zig intended. A session reset erases the codes as well. No fixture changes; a test checks that each code is displayed once and that no page, command or page state holds a code after the acknowledgement.

2026-10-15 (Rust port, traffic dashboard): the traffic dashboard and its period, comparison, request timeline, retained seconds, minute history and rankings panels are ported; their fixtures are byte-identical. Two Zig behaviours change. First, a 401 or 403 reply to a traffic-period, comparison or ranking-history read reset the whole state, including the theme and density, while every other session expiry kept the appearance; the Rust dashboard ends these sessions like every other expiry and keeps the appearance. Second, the Zig

retained-rankings table wrote the raw bytes of a referring host into the page, so a host prefix cut inside a multi-byte character produced invalid UTF-8; the Rust table shows such bytes as replacement characters (a path that is not UTF-8 is still shown as `hex:` digits, as before). Timeline pages, minute pages and summary parts decode with the console protocol's types, which refuse members they do not know where the Zig reflection decoder ignored them. Request serials survive a session reset, as Zig's module variables did, so a reply to an earlier session is never taken.

2026-10-15 (Rust port, investigation pages): the Events, similarity and Challenges pages are ported with byte-identical fixtures. Three Zig defects are fixed. The reply decoder refused every list longer than ten elements, so a page of eleven or twelve per-address challenge records, or of more than ten adaptive-difficulty transitions, read as unavailable although the protocol allows twelve records and thirty-two transitions and the page announces the newest thirty-two; the lists now take the protocol's bounds. A heads reply that arrived after the operator left the Events page left the request loading until sign-out, so no incident's heads could be loaded again; such a reply now forgets the request. The filter form and the source drill-down are checked whole before the query changes, where Zig kept the fields read before the first refused one. The copy-as-cURL command no longer has an 8 KiB bound (a head is at most 2 KiB), and head bytes that are not UTF-8 appear in it as U+FFFD, as the browser showed them. The similarity generation counter still survives sign-out, so a part requested before a sign-out never matches a later search.

2026-10-15 (Rust port, security fixes): the metrics exposition adds `sibuna_bans_refused_total`, `sibuna_forwarded_invalid_total`, `sibuna_honeypot_refused_total` and `sibuna_rate_evictions_total` after the Zig counters.

2026-10-15 (Rust port, policies page): the applied rules, the policy tester, the inspection modes, the managed-rule editor with its review, history, replay, ordering, import and export, the IP groups and the rule hit history are ported; the `policies`, `rule-hit-history` and `rule-hit-history-partial` fixtures are byte-identical, and a differential run that fed 86 events to both modules found no other difference than the fixes below. Replies are decoded when they arrive instead of being kept as JSON text in fixed buffers (4 KiB pages, a 1 KiB decision, a 2 KiB replay, a 2 KiB country summary) that refused larger replies; rule hit parts and the hourly cohorts of a rule decode with the console protocol's types, which refuse members they do not know. Five Zig defects are fixed. The node-local limits sentence was printed into 128 bytes and became "Not reported" when its numbers did not fit (for example 10,000 requests per 60 s with a 600 s ban); it is now printed in full. The IP groups claimed every action named `country-...`, so the globe's buttons that centre a country never worked; the page now claims only `country-preview`, `country-next` and `country-apply`. A refused reputation request kept the success style of an earlier message, and the confirmations of a rule move and of a replaced policy set appeared in the error style, because the message setter cleared the flag set just before it; errors now use the error style and confirmations the success style. A 401 to a reputation request reset the theme and density, unlike every other session expiry; the appearance is kept. A country preview with a malformed review digest stored the preview before refusing it, which enabled the apply button; the reply is now checked first. The audit page opens a recorded policy revision through the action `policies-review-revision` with the rule id and revision, because the audit state belongs to another module; the requests are unchanged.

2026-10-15 (Rust port, consolidation): with every page ported, the interface module built with the old release profile measured 936,750 bytes, above the 768 KiB (786,432-byte) ceiling. It is now built with a dedicated `wasm` Cargo profile (`opt-level = "z"` for every crate, fat LTO, stripped, panics abort; `cargo build -p sibuna-console-ui --target wasm32-unknown-unknown --profile wasm`), and the linker writes call targets and data addresses in their shortest form (`--compress-relocations`) instead of the five padded bytes the LTO object reserves for them. Shared code replaces copies: the command and dispatch helpers take trait objects instead of generic closures, the decision tones, metric names and counter sparkline live in one module, the integer parser and the hexadecimal writer exist once, decimals take a fast path that agrees with the shortest-digits rounding, list decoding is a loop instead of a fallible `collect`, the delta patcher keeps a sorted vector instead of a `BTreeMap`, and one function ends every expired session. The module measures 719,406 bytes (270,612 gzipped), below the ceiling but above the 640 KiB review threshold, which this note records for review; the golden fixtures are byte-identical. The proof-of-work solver built with the same profile is byte-identical to its release build (15,181 bytes), because its hashing crates keep `opt-level = 3`. Six behaviours change. First, every session expiry follows one rule: a 401, or a 403 that refuses the session itself, closes the live connection,

cancels the timers, resets the shared state and every page to the sign-in phase and keeps the appearance (theme and density); some Zig pages reset the appearance, others kept page state or the live connection. The management pages keep answering a 403 with their role message, because there the server refused the action, not the session. Second, the member card's "Consensus address" is now "Management address", the address SID 0013 stores; no fixture shows the card. Third, the console protocol and the interface drop the member fields `applied_slot` and `decided_slot` (SID 0013). Fourth, confirming two-factor authentication drops the session token at once, as Zig did, and the page with the recovery codes stays on screen while signed out until the operator acknowledges them, instead of holding the session in the restricted state of a required enrollment; no request, page or live connection is possible in between, and the behaviour of the previous note is otherwise unchanged. Fifth, a policy set is imported with one request, `policies/import`, whose body is the expected revision and the compact documents (1 to 128 documents of at most 4 KiB, at most 256 KiB in all, the bounds of SID 0013), instead of one request per document and a commit; the review shows the set's SHA-256 over its documents as JSON lines, the digest the `policy.import` audit row names, instead of a client-chosen batch key, the status while the request runs reads "Replacing the rules", and a failed import leaves the set for review again. Sixth, the protocol's events query carries the search text of SID 0013 (`search`, at most 256 bytes); the interface sends none, because the Zig filter form has no search field, and adding one is a change to this record's Events page that awaits review.

2026-10-15 (Rust port, storage calls): the console no longer has a mailbox. Every storage request of the console is a job on the storage thread's bounded queue of 32 jobs (SID 0011), submitted with a ticket. An HTTP handler waits for its ticket at most 10 seconds and then answers 503 `CONSOLEQUORUM`, as before; the job still commits or rolls back whole. The background tasks (the collector with its journals, the hub feeder and retention) never wait: they poll their tickets and hold at most 4 jobs together, counted until each job has run, so at least 28 of the 32 queue slots stay free for HTTP handlers. The mailbox's urgent and background priorities are gone; jobs run in the order they were queued. A full queue answers 503 `CONSOLE003` ("console busy"), where Zig answered 429; a busy password verifier still answers 429 `CONSOLE003`.

2026-10-15 (Rust port, legacy stream): the route `/console/stream` is removed. The interface never used it, and this record specifies only `/console/ws`. A request for it is now an unknown path under `/console/`.

2026-10-15 (Rust port, node storage without consensus): the Rust port has no consensus log, so the storage snapshot of the Nodes page is derived from the database. A SQLite node reports the role `single` and itself as leader; a PostgreSQL node reports the role `unknown` and no leader, because PostgreSQL's failover is not visible to Sibuna. `quorum` means that the node's last database round trip succeeded, and every ballot term is 0. Node rows carry the applied policy revision and no log frontiers. `CONSOLEQUORUM` therefore means "the database did not answer" rather than "the cluster lost quorum". The "leader change" notification bit stays defined, so stored destinations keep their meaning, but no node raises it.

2026-10-15 (Rust port, console router): an unknown GET under `/console/` outside `api/` and `assets/` answers the shell, as the Router section specifies; Zig answered 404. The About reply's `schema` field reports the console schema component's version (1) instead of Zig's schema version 40. `CONSOLEQUORUM` now means that the database did not answer in time, and its hint says so.

2026-10-15 (Rust port, daemon integration): `--console` requires `--data-dir` or `--database-url` (`CONSOLE001` StorageRequired), and `init-admin` is also available as `sibuna console init-admin`. The drain check precedes connection admission in the accept loop. The daemon's build script builds the solver and the interface with the `wasm` profile and `--compress-relocations` and fails the build above 768 KiB; `SIBUNA_CONSOLE_WASM` names a prebuilt module instead.

2026-10-15 (Rust port, rule observations): rule-hit counters are allocated with each published engine (one `Arc` with the engine) and numbered per boot by the publish hook; a refused snapshot publishes nothing, so live counters are never reset. The collector samples the published engine's counters once per second through `Node::sample_rule_hits`. At a publication, the retired generation's open frame is sealed as a cutover, which is never complete. The new generation's first interval starts at its publication when that time is at most five seconds before the first sample; otherwise it starts at the first sample, and earlier hits are counted as unconfirmed.

2026-10-15 (Rust port, ban gauge): the active-ban gauge is a relaxed counter of slots whose expiry is non-zero, kept by an atomic swap or compare-exchange on every expiry change; each gauge read sweeps one

sixteenth of the table and zeroes expired expiries. It never misses a ban in effect, lags an expiry by at most sixteen reads, and never takes the writer lock that request threads use.
2026-10-15 (Rust port, collector): the collector thread runs every 250 ms and reaches storage only through background tickets, within the console's allowance of four jobs. A journal write that cannot be queued is tried on the next tick without spending a retry. A job unanswered after ten seconds is abandoned and counted as unconfirmed. Journals no longer prune: the retention job deletes minutes, ranking archives and challenge records under its lease (SID 0013), and failed retention batches of minutes and rankings appear as those journals' maintenance failures. The ranking journal reads the archive inventory every five seconds and stores each archive in one step.
2026-10-15 (Rust port, membership and gauges): membership rows are announced by the collector at start, every minute, and within two seconds of a change of the applied policy revision or the control revision. Resident memory and CPU time are read from `/proc`, with a CPU resolution of 10 ms. `geo_maintenance_failures` is always 0, because GeoIP pruning is a retention kind.
2026-10-15 (Rust port, access): a refused sign-in is audited (`session.denied`) before the 401 reply instead of through a background mailbox job; the reply stays identical for an unknown account, a wrong password and a wrong second factor. Unknown accounts are verified against a constant PHC string with the console's Argon2id parameters, so they cost a full verification. The single Argon2id workspace (19 MiB) is allocated at start and wiped by every use; a concurrent check is refused with 429 `CONSOLE003`. Storage failures of sign-in, password change, TOTP and kiosk exchange answer 503 `CONSOLEQUORUM`. The `sibuna console` client speaks HTTP/1.1 through `sibuna-tls` (plain HTTP only to loopback literals), bounds replies to 16 KiB and each request to 20 s, never follows redirects, and imports a policy set with one `policies/import` request.
2026-10-15 (Rust port, node commands): the intent commits first; the console checks authority and expiry again before the local effect, which runs through the daemon's `Node` trait; a completion that cannot be recorded is kept in memory, retried by the next request and by the collector, and blocks new commands; a command arriving while another runs is refused with 503 `CONSOLENODE` instead of queueing. The policy page reads the engine the node serves through `Node::engine`; the policy tester without a draft and replay evaluate the committed policy composed by storage, reported beside the node's applied revision.
2026-10-15 (Rust port, live hub): the hub keeps its bounds (rings of 1,024 records of at most 2 KiB per topic, outboxes of 64 frames, views of 64 KiB and filtered views of 16 KiB) but allocates them on demand. A ring is guarded by the hub's topic lock, so a publication is never lost to contention; Zig reported such a loss as a one-record gap. Server messages carry only the members of their operation, in the order of this record's example, which the console reproduces byte for byte; Zig also wrote `"data":null` and the unused part, update and kind members. Fan-out runs once per second on the first feeder tick of each new second of the console's clock. A stream writer waits on its subscriber's condition variable for at most 100 ms instead of sleeping 100 ms. If the five-second recheck cannot reach storage, the stream closes with 1013 instead of reporting the session unauthorized. The feeder reaches storage only through background tickets and holds at most two of the console's four background jobs.
2026-10-15 (Rust port, notifications, GeoIP and probes): the notifier runs on its own thread with background storage jobs inside the console's allowance of four, waiting at most 10 s for each; it renews the lease before every claim, and an attempt's 20 s budget is measured from before the renewal. Webhooks use the console HTTP client over `sibuna-tls`; the checked address is pinned, plain HTTP is allowed only to loopback literals, and the reply body is read up to 64 KiB (a larger body fails the attempt). GeoIP downloads resolve publisher hosts under the public-only policy and pin the connection; one HTTPS redirect is allowed, to the provider's asset host. The embedded snapshot reaches the console as `Inputs::geoip_embedded` and is decoded once at start when storage has no generation. Restore reads 64 chunks per transaction. An operator checksum must be hex, and oversized import fields answer 400.
2026-10-15 (Rust port, prompt stop): the console's outbound I/O for webhooks, syslog over TCP, GeoIP downloads and data-plane probes never blocks in one socket operation for more than 250 ms. After each slice it checks the deadline and the console's stop flag (for an import, the importer's cancel flag). The TLS handshake follows the same rule through `Connector::connect_cancellable`. Connection attempts start at 250 ms and double up to 1 s, so a distant server can still answer. Stopping therefore ends a delivery, download or probe in flight within about a second, instead of waiting for the 10-second delivery deadline or the 120-

second download deadline. Zig cancelled the I/O task directly. Name resolution is the exception: it waits for the system resolver, which its own configuration bounds.
2026-10-15 (Rust port, management peers): outbound peer workers read with a socket deadline of at most 250 ms and poll between reads, so queued queries are sent, the console's stop is noticed, and the 10-second progress deadline and one-hour cap are enforced without a cancelling task. The peer query mailbox is a queue of owned queries per peer (at most 8 outstanding) with a condition variable per caller; a query whose caller gave up is skipped instead of sent, and queued queries are cancelled when the console stops. A query answer must fit one 4 KiB WebSocket message: the serving console halves the rows of a page that does not fit and answers `unavailable` when one row does not; Zig closed the stream. A refused certificate marks the peer `rejected`, like a refused proof. The inbound `/console/peer` stream shares the browser stream's writer and reader, as a peer party limited to unfiltered local statistics and queries.
2026-10-15 (Rust port, oversized events): the browser bridge no longer drops an event longer than the module's input bound (`INPUT_LIMIT`, 101,168 bytes, kept because it bounds the parsed event tree). It replaces the event with a small one: a server reply fails as a network error does (status 0); a stream message counts as invalid, so the connection restarts; any other event, in practice a large form, arrives as event kind 11 with the refused kind, its action name (at most 128 characters) and its length. The policies page answers a refused policy set with "The policy set is larger than this page accepts. Import it with sibuna console policies import –file <set.json>.", since the import request allows 256 KiB (SID 0013); any other form gets "This form is larger than the console accepts. Shorten it and try again." Both messages take focus. The policy set field no longer has a `maxlength` of 65,536, which cut a longer paste short without a message, and its note names the command-line import for sets above about 96 KiB. Zig's bridge dropped such events silently, so a large pasted policy set was ignored and an oversized reply left its request pending.
2026-10-15 (Rust port, daemon wiring): the daemon passes the console its policy base (WAF switch, policy file, global limiter, honeypot ban and its own challenge interstitial), the served engine, its open data-plane connections (shown by `nodes/local`), and node id 1 when `--cluster-node` is absent, as the storage thread numbers the node. `--console-query-steps` is part of the console configuration and bounds every aggregate read. Rule observations: the engine slot keeps the counters of the generation the console last sampled until the next sample has read their final values, so a publication loses no hit counted before that read. A hit that a request records into the retired counters after that read is not counted. A build may embed one GeoIP snapshot named by `SIBUNA_GEOIP_DATA`, decoded at build time; a build without the console refuses one (`GEOIP001`). `sibuna console` writes GeoIP progress and the sign-out warning to standard error.
2026-10-15 (Rust port, GeoIP loader): a `sibuna-geoip` loader is spent after its first error, and every later call returns that error. Decoding a replicated batch of ranges appends nothing when a row is bad, where Zig kept the rows before it, and encoding a batch of more than 100 ranges is an error, where Zig asserted. `sibuna-inflate` reports a truncated DEFLATE stream as a corrupt archive; Zig 0.16's decoder panicked with an integer overflow on some truncated streams in safety-checked builds. It also refuses an input that is not gzip as soon as the magic, method or flags byte arrives, where Zig reported the end of the stream.
2026-10-15 (Rust port, console cryptography): the XChaCha20-Poly1305 of seed envelopes comes from `sibuna-crypto`. Opening checks the tag first and then decrypts in place, so a refused envelope leaves its ciphertext in the buffer; Zig decrypted into a separate buffer and left it undefined. A message too long for the construction is an error where Zig asserted. AEAD keys and the ChaCha20, Poly1305 and keyed BLAKE2b states are wiped when dropped. PHC verification reports an unknown algorithm as unsupported, where Zig reported a failed verification, and a salt or hash longer than 64 bytes as an invalid encoding, where Zig reported a full buffer. `hash_phc` takes the salt from its caller, because the crate has no source of randomness; the console draws 32 random bytes for it, as Zig did inside the hash function.

2. Abstract

Specifies the Sibuna Console, a complete management interface for Sibuna: a separate pure-Zig module started from the Sibuna CLI that serves a real-time web interface over the standard library's HTTP server and WebSockets, renders its pages from a WebAssembly module styled with daisyUI 5, keeps authentication, statistics, audit, and a GeoIP database in the embedded Zaxonlite store, manages one node or a replicated cluster, and defines performance acceptance targets that remain to be measured.

Command-line flags, JSON policy files and the embedded Zaxonlite store support Sibuna deployment and automation. Operators also need a web console: a statistics overview with live traffic and attack charts, an attack-event browser with payload detail, rule editors, address groups, and system settings. This record specifies the Sibuna Console: a proposed first-party Zig module, compiled into the same binary and started from the Sibuna command line, that provides that class of interface for one node or a replicated cluster. The console serves HTTP and WebSockets with the Zig standard library, renders every page from a WebAssembly module written in Zig and styled with daisyUI 5 through first-party components, streams statistics and events in real time, and keeps users, sessions, audit records, minute-level statistics, and a GeoIP country database in the same Zaxonlite store the data plane already replicates. Its interface is designed by three principles applied page by page: Krug's "don't make me think", support for fast System 1 judgement, and support for deliberate System 2 analysis. Its defining engineering constraint is an isolation contract: the console may read the data plane's counters and its database, and it may write the database, but it never enters a request thread, never allocates on one, and never holds a lock a worker needs; a proposed benchmark gate checks that the console's presence degrades data-plane throughput by at most one percent and p99 latency by at most ten percent under the specified workloads. These are proposed acceptance targets, not measured results.

Status and applicability

This architectural discussion defines requirements and their rationale. Proposed targets are not measured guarantees. Zig 0.16.0 and Zaxonlite 0.6.2 are the implementation baseline. The service and interface logic are Zig; browser glue and committed CSS supply host capabilities and styling. Storage links SQLite and libc as described in SID 0005. Only browser modules target `wasm32-freestanding`.

3. Introduction and Motivation

SID 0002 defines the Gate and Shield surfaces, SID 0003 the declarative policy, SID 0004 the inspection engine, and SID 0005 the storage layer with dynamic policies, replicated reputation, and forensic incident search. SID 0005 closed with an open item: "an authenticated HTTP administration API for policies and incident search." Operator questions illustrate that gap. How much traffic did the gate challenge in the last hour, and how many challenges were solved? Which addresses were banned on which node, and did the ban propagate? Which rule fired for a denied request, and what did the payload look like? Is node 2 the leader, and is it healthy? Some answers exist in Prometheus counters and `security_incidents`; others require new instrumentation and a storage-status API. The console must distinguish measured values, sampled estimates, missing evidence, and planned capabilities.

Sibuna operators need a front page that explains current traffic and protection outcomes, an investigation path from a denial to recorded evidence, and controlled editing of policies, address groups, users, retention, and notifications. These workflows must reflect Sibuna's surfaces, policies, and nodes, including challenge verification, cluster membership, and campaign investigation. Missing evidence must remain visibly unavailable.

4. Operator Workflows

The interface uses a labelled left sidebar, a top bar with a breadcrumb, theme and refresh controls, and a page body. Lists provide relevant filters, refresh controls, bounded exports, and pagination. Incident details distinguish recorded request evidence from absent response data. The following requirements describe the proposed Sibuna workflows.

Workflow	Operator requirements
Traffic statistics	Select time range and nodes; inspect requests, admitted, challenged, denied, distinct banned addresses and origin 4xx/5xx counts. View a live globe, country ranks, timeline and sampled request rankings with loss and coverage metadata. Page views and unique visitors require separate instrumentation.

Workflow	Operator requirements
Security posture	Inspect trends and source addresses for inspection, reputation, rate limiting, challenges, bans and honeypots; follow live events, attack categories and attacked paths. Show each decision with its recorded reason.
Wall display	Open a read-only, scoped, expiring kiosk session with the globe, country ranks and module trends; keep payload evidence outside the kiosk scope.
Nodes	Inspect each node's surface, upstream, listener, traffic, health and applied revision. Sibuna protects one origin per process. Preview drain and clear-local-bans commands and inspect their completion.
Attack investigation	Browse grouped and raw incidents, filter and paginate, export bounded results, and inspect redacted request evidence. Show rule evidence, available scores, campaigns and similar incidents. Historical fields absent from storage say "not recorded"; JA4 requires bounded capture from a trusted ingress that overwrites spoofed headers.
Inspection controls	Set each supported category to disabled, audit or enforce. Audit records findings and continues evaluation, preserving other enforcing denials. Category modes extend the current global inspection switch.
Rules and address groups	Edit and order rules, test a private candidate engine, import/export, inspect history and revert with revision checks. Manage reputation prefixes, groups and country-derived prefixes within existing engine capacities.
Rate limits	Inspect configured and effective node-local limits, their outcomes and affected addresses. Terminal-rule GCRA extends the existing global limiter; reject limiter settings on WEIGH rules. Overload remains visible through challenges and bounded-connection rejection.
Challenges	Inspect issued, submitted, accepted and rejected solutions, rejection causes, solve-time distributions and missing timing coverage. Display configured difficulty and effective proof parameters separately.
Operational settings	Manage constrained blocking/challenge templates, retention, bounded webhooks and syslog, GeoIP generations and About information. Show storage and cluster coverage without inventing healthy or zero states for missing nodes.
Console access	Manage users, roles, password changes, TOTP/recovery, scoped API tokens and revocation. Keep the authentication shell separate from dashboard data and geometry.
Audit	Investigate redacted console mutations, revision conflicts and changes; show local-command intent and completion separately.

Authenticated pages share one WebSocket with snapshot/delta streaming; the backend polls storage and health endpoints. Bounded request samples feed request-level rankings. Page views and unique visitors cannot be inferred accurately from these samples and are excluded unless separately instrumented. Incident details expose recorded rules, available scores, campaign membership, and similar incidents while marking missing or truncated evidence.

The design follows the approach the zenfmt project uses for its server interface: a bounded service kernel over the standard library, an application layer that composes routing, authentication, and handlers as straight-line code, a WebAssembly interface module in Zig that owns every page and all interface state, a fixed JavaScript glue that only moves events in and commands out, and vendored daisyUI styling. Sibuna's console has eight navigation sections, live streams and a cluster, so the module structure below is deliberately more granular, and the transport is WebSockets rather than server-sent events because the interface also sends commands (subscribe, filter, acknowledge) on the same connection.

5. Design Principles

Three principles govern every page, and the principle audit audits each page against them. They are not decoration: each yields testable rules (R1 to R18) that the verification section checks.

5.1. Don’t make me think

Krug’s rule is that a page should be self-evident: a person should know what it is, what they can do, and where they are without reading. Applied to a security console, whose operator is often looking at it under pressure, the rule becomes:

- **R1 One question per page.** Every page answers one question stated in its title: “What is happening?” (Statistics), “What was attacked and why?” (Attack events), “Are the puzzles working?” (Challenges), “What are the rules?” (Policy), “Is the cluster healthy?” (Nodes). Observation pages have useful defaults (all nodes, last 24 hours, live on); mutation forms explicitly ask for the information and confirmation they need.
- **R2 The trunk test.** From any page, without scrolling, the operator can name the product, the cluster and node, the page, the section within it, and the way back: the top bar and breadcrumb carry all five, always in the same place.
- **R3 Conventions over invention.** A left sidebar of pages, a filter bar above every list, a detail on the right, primary actions top right, destructive actions red and confirmed. Sibuna’s own vocabulary (Gate, Shield, Edge, work bits) appears with a plain-language gloss on first use per page, never a tooltip the operator must discover.
- **R4 Obvious clickability.** Every clickable thing looks clickable and nothing else does: links are coloured and underlined on hover, buttons are buttons, table rows that open a detail show a chevron. No hidden gestures, no right-click menus, no double-click.
- **R5 Omit needless words.** Labels are nouns, buttons are verbs, and both are short. Intro banners, marketing copy, and explanations of what a firewall is do not appear; the one explanatory line a panel may carry links to the book.
- **R6 Nothing moves that does not need to.** Tiles and charts update in place at 1 Hz with no animation; new rows accumulate behind a “Show new events” control whenever the reader has scrolled or focused a row; layout never reflows on data.
- **R7 Errors are Elm-style.** A failed action names what happened, why, and what to do, in the diagnostic voice the daemon already uses, inline where the action was taken.

5.2. Fast judgement: System 1

Kahneman’s System 1 is fast, automatic, and pattern-driven; an operator glancing at the console should be able to notice a potential anomaly quickly; these are usability goals to test with operators, not guarantees of correct judgement. The interface therefore invests in preattentive cues and consistency:

- **R8 One colour per decision, everywhere.** Admitted is green, challenged is amber, denied is red, banned is dark red, informational is the single blue accent; the same hue in tiles, chart series, badges, and rows, in both themes. Decision badges keep these meanings; health uses separate labelled status icons, and charts never rely on colour alone.
- **R9 Deviation, not magnitude.** Each tile shows its value and a small marker of how it compares with the same window yesterday (an arrow with a percentage), because a raw count is meaningless at a glance and a change is not. A tile whose deviation exceeds a threshold gets a tinted background. Compare equal-duration windows with matching coverage; zero prior counts show “new”, and absent history shows “not available”, never an infinite percentage.
- **R10 Stable positions.** A panel is always in the same place at the same size; rankings keep slots and update bar length without animation; the map keeps its projection. Recognition works by location as much as by shape.
- **R11 Sparklines beside numbers.** Every count that has a history shows a 60-point sparkline next to it, so a spike is seen before it is read.
- **R12 Scannable typography.** Numbers use tabular figures and thousands separators, are right-aligned in tables and large in tiles; addresses and identifiers are monospaced; relative times (“12 s ago”) in live views and absolute times in logs.
- **R13 Semantic icons only.** One icon per module (inspection, reputation, limits, challenge, ban, honeypot, node), used consistently; no decorative icons.

5.3. Careful judgement: System 2

System 2 is slow, effortful, and analytic; it is what an operator engages when deciding whether to ban a network, change a rule, or declare an incident. The console supports it by making evidence explicit and decisions reversible:

- **R14 Evidence for every conclusion.** A denial shows its recorded reason and evidence; score terms, matched spans and raw request fields appear only when captured, otherwise "not recorded"; a challenge shows its parameters and recorded outcome; a ban shows who or what caused it and when it expires. No verdict appears without its reason.
- **R15 Depth on demand.** Pages are layered: glance (tiles), scan (tables), study (detail modal), investigate (campaign members, nearest incidents, the same address across nodes). Each layer is one click deeper and the way back is always the same control.
- **R16 Compare, don't recall.** Any period can be compared with the previous one, any node with another, and any rule's hits before and after an edit; the interface places the two side by side so the operator never holds one in memory.
- **R17 Simulate before you commit.** The policy tester evaluates a synthetic request against the current policy; a rule edit shows a diff of what will change and which recent events it could have matched from retained inputs, before Save. Truncated or absent inputs make a replay inconclusive; the tester does not reproduce live rate-limit, ban, or token state.
- **R18 Reversible by default.** Bans and allows carry a duration and an "undo" for thirty seconds; rule edits are versioned and can be reverted from the audit page; deletion needs a typed confirmation; drain and broad country changes require an impact preview and confirmation. Undo is a new versioned mutation, not deletion of the audit record.

5.4. Elegance

Elegance is the absence of anything unnecessary, not the presence of ornament. The visual system is small enough to hold in one's head: one accent colour and the four decision colours; a neutral surface scale of five steps per theme; one typeface for text and one monospaced face for identifiers, in a five-step type scale (12, 14, 16, 20, 28 px); an 8-pixel spacing unit; 4-pixel corner radius on inputs and 8 on cards; one shadow level for overlays only; 150 ms transitions on hover and none on data. The daisyUI theme `sibuna` is defined once from these tokens and the `sb-*` components use nothing else, so the console looks like one thing rather than a collection of widgets. Density is a preference (comfortable or compact) remembered per browser, because the same operator wants air on a laptop and rows on a wall display.

5.5. Principle audit by page

Page	Don't make me think	System 1	System 2
Statistics / Traffic	Answers "what is happening?" with defaults: all nodes, 24 h, live. No selectors demand attention until needed (R1, R2).	Six tiles with deviation markers and sparklines; one stacked timeline; decision colours throughout (R8 to R11).	Period comparison toggle; every tile drills into its table; sampled panels say "sampled" (R15, R16).
Statistics / Security	One row of module tiles, one trend per module, the live feed on the right; the same layout as Traffic so the eye does not relearn (R3, R10).	Trends share a y-axis so a spike in one module reads against the others; the feed uses module icons and decision colours (R8, R13).	Each trend opens its module's events filtered to the period; the feed row opens the detail modal (R14, R15).
Attack events	Two views named for what they group (by source, raw); one filter bar; one detail control (R1, R4).	Category chips coloured by decision; country flags; new rows wait behind the reader-controlled update button (R6, R8).	The detail modal is the System 2 workbench: rule, score terms, decoded payload, raw request, campaign, nearest incidents, and the actions with durations and undo (R14, R17, R18).

Page	Don't make me think	System 1	System 2
Challenges	The funnel is the page; nothing else competes with it (R1, R5).	Funnel stages in decision colours; the histogram shape shows a slow-device tail at a glance (R8, R11).	Per-cause rejection tables; difficulty bump timeline against load; per-rule parameters editable with a preview of expected solve time (R14, R17).
Policy	Rules read top to bottom in evaluation order, with the order shown as a number and drag handles; one editor (R3, R4).	Type chips in decision colours; hits-today sparkline per rule; disabled rules greyed (R8, R11).	Tester, diff before save, "would have matched" against recent events, versions with revert, inspection-mode matrix with a one-line consequence per mode (R16 to R18).
Nodes	One card per node; leader marked; unhealthy first (R1, R10).	Health as colour plus word; sparklines for rate, memory, CPU (R8, R11).	Per-node drill to its statistics; replication lag history; drain with a confirmation that states what it does (R14, R18).
Settings, GeoIP, Audit	Tabs named by noun; forms with one primary action; nothing hidden behind icons (R3, R5).	Two-factor state and token expiry as badges; retention as a sentence, not a table (R12).	Audit rows show before and after; page templates preview live; GeoIP shows source, licence, and count before the update button (R14, R17).

6. Terminology and Scope

- **Data plane**: the Sibuna daemon's request path (accept, parse, classify, verify, proxy), its worker and connection threads, and its bounded tables (including the sharded, locked spent set).
- **Storage thread**: the existing thread of SID 0005 that owns the Zaxonlite node and rebuilds engine slots.
- **Console**: the management application specified here: its listener, threads, module, and tables.
- **Kernel**: the console's bounded HTTP and WebSocket service layer (`libs/serve`).
- **Interface module**: the `wasm32-freestanding` Zig module that renders pages in the browser.
- **Glue**: the fixed JavaScript file that loads the module, opens the WebSocket only after authentication, forwards events, and executes commands.
- **Topic**: a named real-time stream (`stats`, `events`, `nodes`, `policy`, `challenges`, `audit`).
- **Node**: one Sibuna process; **cluster**: the Zaxonlite member set of SID 0005.

In scope: everything needed to observe and manage one node or a cluster from a browser and a JSON API. Out of scope: TLS termination for the console (an ingress terminates it, as for the data plane), per-site upstream routing (Sibuna proxies one origin per process), payment or licensing, and mobile-native clients.

7. Goals and Non-Goals

7.1. Goals

- One binary, one command: `sibuna --console 127.0.0.1:9443` starts the console beside the data plane; `-Dconsole=false` compiles it out entirely.
- A complete management surface for everything Sibuna does: statistics, events, challenges, policy, reputation, nodes, GeoIP, users, tokens, pages, retention, notifications, audit. The console is complete on its own terms: one product, one feature set, no editions.
- Designed by three principles, applied and audited per page (Design Principles): don't make me think; fast, glanceable judgement (System 1); deliberate, evidence-backed analysis (System 2).
- Elegant: one accent colour, one type scale, one spacing unit, restrained motion, and nothing on a page that does not earn its place.
- Real-time by default: the overview targets 1.25-second counter-to-display updates; incident delivery is subject to storage backlog, commit time, polling, and broadcast delay.

- Cluster-aware: one console shows configured members and marks unobserved members; policy and reputation edits made on any node reach every node through the replicated tables of SID 0005.
- Pure Zig: the kernel, the application, and the interface module are Zig; the only JavaScript is the fixed glue; the only CSS is daisyUI 5 plus first-party components.
- The isolation contract in "Process model and the isolation contract", with a measured gate.
- Every build product, including the stylesheet built by npm, is produced by `zig build`.

7.2. Non-Goals

- A general dashboard framework or plugin system.
- Replacing Prometheus: the console reads the same counters and leaves `/__sibuna/metrics` untouched.
- Editing the JSON policy *file*: the console edits the replicated `policies` table, which precedes file rules by design (SID 0003); the file remains the bootstrap.
- Geo-blocking as a data-plane feature. GeoIP enriches events and statistics in the console and can feed `ip_reputation` rows through an explicit operator action; the request path never consults it.

8. Architecture Overview

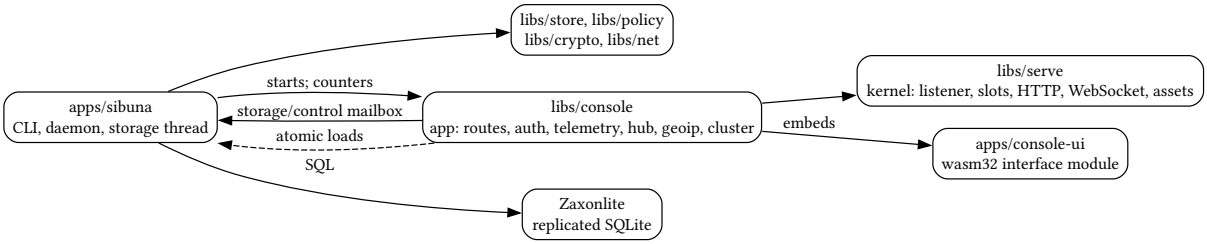


Fig. 2 Proposed modules and runtime interfaces. The daemon owns database access; console work uses its bounded mailbox. Dashed telemetry reads do not take engine or request-state locks.

8.1. Modules and directories

Path	Contents
`libs/serve/src/`	Bounded listener and connection lifecycle in `kernel.zig`; request/response context, admission quotas, WebSocket framing, upgrade and I/O. The application supplies routes and static assets.
`libs/console-protocol/src/`	Bounded application values, roles, storage/control operations, subscription messages, history arithmetic and browser contracts. Builds natively and for Wasm without networking, storage or daemon imports.
`libs/console/src/`	Application routing and authentication; telemetry aggregation, subscription hub, peer transport, GeoIP activation and management services. SQL execution remains behind typed owner requests.
`apps/console-ui/src/`	Wasm ABI, application state and controllers, page renderers, shared components and SVG charts. HTML snippets express markup through the bounded `libs/html` renderer; native golden tests exercise the same renderers.
`apps/console-ui/web/`	Authentication shell, fixed browser bridge, Tailwind source, pinned asset tools and committed CSS/geometry. Ordinary builds consume committed assets without npm.
`apps/sibuna/src/`	Composition, console-specific CLI parsing and subcommands, startup/shutdown, storage mailbox execution and immutable policy publication. `AppState`, engine ownership and `Persistent` remain daemon responsibilities.

The service kernel has no firewall or database knowledge. Console services use library-owned contracts and import nothing from `apps/sibuna`; the daemon composes these services and supplies metrics, bounded telemetry and the storage-command mailbox. Shared metrics live in `core`; incident samples cross a bounded `store` tap, while the daemon retains its durable incident queue and adapts storage results into protocol values. There is no database-handle factory. The storage thread remains the sole owner of `Persistent`, its allocator and database facade. Console SQL work is serialized through that mailbox with priorities, result-

size bounds and per-tick quotas; it must not call `rebuild` or `publishEngine` itself. Heavy forensic queries need validated cancellation/deadlines or a separately owned read snapshot before release. An arbitrary SQLite connection must not bypass Zaxonlite's commit/replication path.

8.2. Process model and the isolation contract

The console runs on its own listener and bounded threads, with explicitly owned buffers and scratch arenas. It shares the process and its CPU/cache/memory bandwidth with the data plane, plus controlled storage, metric, telemetry and command interfaces. The contract is stated as invariants and each has a test.

Invariant I1

No console code executes on a data-plane worker or connection thread. The daemon's `dispatch` has no console branch; console routes live on the console listener.

Invariant I2

The console reads data-plane state only through atomic loads of `Metrics` and through bounded storage requests, plus the explicitly proposed telemetry rings. It never takes a shard spinlock, pins an engine slot, or consumes the incident ring.

Invariant I3

The console writes data-plane state only through the database. A policy or reputation change is a committed row; the storage thread's existing tick observes the revision and publishes a rebuilt engine exactly as SID 0005 specifies.

Invariant I4

Console-owned memory has explicit capacity and admission bounds: the connection slots, the WebSocket ring, the subscriber table, the sampler's minute buffers, and the GeoIP range array have fixed capacities recorded in `console.Budget`, and the sum is printed in the startup banner, including thread stacks (each service thread reserves its usable 256 KiB plus the 256 KiB per-thread signal stack that glibc places in static TLS, without which Linux refuses the thread), request bodies, authentication workspaces and double-buffered GeoIP reloads. Database/cache memory is measured separately as part of process RSS.

Rust port note (2026-10-15)

The Rust service threads reserve the usable 256 KiB without the separate signal-stack term, because the Rust standard library maps its signal stack itself. See the revision note.

Invariant I5

Console work is rate- and size-limited: the sampler runs at 4 Hz, broadcasts are coalesced to 1 Hz per topic, event fan-out is capped at 64 records per second per subscriber, and the GeoIP loader uses bounded batches. This does not provide a hard CPU-time bound: SQL, hashing, scheduling and shared cache/memory bandwidth still require measurement.

Invariant I6

Recoverable handler, database and capacity errors fail console operations without stopping the request listener. A Zig panic, memory corruption, or process OOM can terminate both planes: a shared process

is not a fault-isolation boundary. A separate console process is required if crash isolation becomes a requirement.

I3 has two explicit control exceptions: drain and clear-local-bans use a bounded, authenticated command mailbox consumed by data-plane control code. Console threads never mutate ban-table internals. Both commands require an audit intent, operation id and completion record, since a local effect and a database transaction cannot be committed atomically.

Enabling the console must not add shared-cache traffic to the request path. Per-request console telemetry is therefore striped across sixteen 64-byte counter lines: each connection thread selects one stripe when it seeds its sampler, the rule-hit counters are striped the same way, and readers sum every stripe. User-Agent classification and referer parsing run only for the one request in sixty-four that the sampler already selected. Without this an enabled console cost three to four and a half percent of throughput, through one shared atomic add per request, a compare-and-exchange loop per matched rule, and classification of every request.

The impact gate compares console compiled out, compiled in but disabled, idle, and eight active dashboards. Measure admitted, challenge, denied/incident-heavy and policy-reload workloads, including authentication and GeoIP reload contention. Use repeated interleaved runs on a declared host, fixed warm-up/duration and traffic mix, and report uncertainty. Throughput loss must be $\leq 1\%$ and p99 increase $\leq 10\%$ relative to the corresponding baseline; inconclusive/noisy runs do not establish compliance.

The owner accepted a supplementary paired reading of the September 2026 measurements (decision of 14 September): comparing idle and active consoles with the same binary disabled, within each round, suggested at most 0.8% runtime cost without capture for single nodes and 0.5% for the local cluster. This was an exception, not a pass: the single-node formal verdicts were inconclusive and the clustered verdict failed against the compiled-out binary. Those measurements predate the request-path changes of 1 October and remain historical evidence. They do not establish compliance for later code or authorize an exception for new results.

The October review measures the updated request path in unprivileged Linux containers. Three physical hosts run mutual-TLS consensus and certificate-validated management peers; the fixture verifies all six peer directions and eight dashboards, including rankings and retained timeline queries. The quiet forward-auth/capture-off repeat and the other three mode/capture matrices are selected by `benchmarks/results/console-impact-three-host-*-latest.json`. All have valid response states, dashboard delivery and peer coverage, with no transport errors, but formal verdicts are inconclusive. The quiet repeat's baseline spread is 2.5 to 3.9%; its active throughput loss is 1.5 to 3.4% against compiled out and 0.9 to 3.5% in the supplementary paired comparison with disabled. The initial forward-auth/capture-off matrix is exploratory because another fixture shared node 3's physical host. Timestamped records preserve both runs and their provenance.

Four current single-node matrices cover both modes with capture off and on, verifying all 360 sample response states and eight-dashboard delivery and query coverage without transport or subscription errors. Their formal verdicts are inconclusive, with baseline spread of 0.9 to 7.4%; even a steadier workload remains inconclusive when its uncertainty interval crosses the gate. All 54 non-baseline configuration comparisons in each topology are inconclusive. The five core benchmark families were regenerated for the same application revision and pass their functional checks. The combined evidence, record digests and verified cleanup are in `benchmarks/results/linux-launch-review-20261002.json`. None of these isolation measurements is a formal pass.

These containers cannot control the processor governor or other host activity. That limits acceptance; it does not establish that every measured difference is noise. Linux `ps` CPU time is quantized to whole seconds, whereas throughput and latency use the independent load generator clock and histogram. The latter measurements are not explained away by coarse CPU accounting. The thresholds above remain the contract. Results and fixture provenance belong in `benchmarks/results/`; this record states their implications for the design and launch.

8.3. Startup from the command line

```
sibuna --console 127.0.0.1:9443 --data-dir /var/lib/sibuna --secret-file /etc/sibuna/secret
sibuna --console 0.0.0.0:9443 --console-behind-proxy --console-cookie-secure ...
sibuna --console 127.0.0.1:9443 --console-advertise https://console-1.example \
  --console-probe 2=http://10.0.0.2:8080 --console-probe 3=http://10.0.0.3:8080 ...
sibuna console init-admin admin --data-dir /var/lib/sibuna
sibuna console add-user alice --role viewer --origin https://console.example \
  --username admin --password-file /run/private/console-password
sibuna console users --origin https://console.example \
  --username admin --password-file /run/private/console-password
sibuna console geoip status --origin https://console.example \
  --username admin --password-file /run/private/console-password
sibuna console geoip update --month 2026-09 --origin https://console.example \
  --username admin --password-file /run/private/console-password
# Optional: --checksum <compressed-source-sha256> --timeout <seconds>.
sibuna console mint-token monitoring --scope stats_read --scope geoip_read \
  --origin https://console.example --username admin --password-file /run/private/password
sibuna console tokens --origin https://console.example \
  --username admin --password-file /run/private/password
sibuna console revoke-token 42 --revision 1 --origin https://console.example \
  --username admin --password-file /run/private/password
sibuna console geoip status --origin https://console.example --token-file /run/private/token
# mint-token: optional --role and --expires <absolute Unix seconds>.
# remove-token explicitly removes inactive metadata, retaining the audit trail.
```

`--console` requires `--data-dir` and storage support (`-Dconsole=true` with `-Dstorage=false` is a build error; the console default follows storage): users, sessions, and statistics live in the database, and a console without persistence would lose its administrator on restart. The console listens on loopback by default; binding elsewhere without `--console-behind-proxy` (which requires an explicit trusted-proxy CIDR list and canonical HTTPS console origin) is refused. Only allowlisted socket peers may supply forwarded address or scheme headers; the ingress strips client-supplied copies. Proxy mode enables `Secure` cookies. HTTP on loopback is development-only. Account, token, GeoIP and policy import/export operations have CLI clients; other management workflows use the authenticated interface or API. Offline bootstrap takes an exclusive data-directory lock; commands against a running node use the authenticated console API, never a second embedded node over the same directory. In a cluster every member may run a console; each shows the whole cluster, because the tables it reads are replicated, and each probes the others' health endpoints directly.

9. The Serve Kernel

`libs/serve` is a bounded service kernel over `std.http.Server` and `std.Io`. It is the console's HTTP substrate, not an OS kernel, and is written to be reusable by a future service; it knows nothing about firewalls.

- **Listener and slots.** One acceptor thread; `max_slots` (default 96, at most 256; reserve at least 16 slots for HTTP and control traffic) connection threads with fixed 16 KB receive and send buffers. A head larger than the receive buffer is `431`; a full slot table is `503` with `Retry-After`. Deadlines (head 10 s, idle 60 s, body 30 s) are enforced by a watchdog thread that shuts down expired sockets, the same mechanism the daemon's idle reaper uses, because the threaded `std.Io` exposes no per-read timeout.
- **HTTP.** `std.http.Server.receiveHead` parses the request; `Request.respond` and `respondStreaming` write responses. Bodies are limited to 1 MB except the policy import route (8 MB). Every response carries `Cache-Control`, `Content-Security-Policy` (`default-src 'none'; script-src 'self' 'wasm-unsafe-eval'; style-src 'self'; img-src 'self' data:; connect-src 'self'; object-src 'none'; base-uri 'none'; frame-ancestors 'none'; form-action 'self'`; add only the exact console WebSocket origin if required by a supported browser), `X-Content-Type-Options`, `Referrer-Policy`, and `X-Frame-Options`.
- **WebSocket.** `Request.upgradeRequested` and `respondWebSocket` provide the Zig 0.16 handshake/writer primitives. `readSmallMessage` is bounded by its input buffer, not a built-in 4 KB constant, and rejects fragmentation. The kernel must implement and test RFC 6455 fragmentation, masking, RSV/opcode checks, UTF-8, control-frame limits and close handling; cap a reassembled client message at 4 KiB (1009 on overflow). Each connection has independent read progress and one serialized writer, so blocked reads do not prevent unsolicited statistics delivery. Ping/pong and close frames share that writer. Bound write time, close idle peers, and account both tasks/threads in the memory budget.

- **Assets.** Embedded files (`shell.html`, `glue.js`, `console.css`, the interface module, `world-110m.bin`) are served under `/console/assets/<sha256-prefix>/<name>` with `Cache-Control: immutable`; the shell's placeholders resolve at start to those paths, so a new build names its assets by content; serve the shell with `no-cache`, immutable assets with `max-age=31536000`, and sensitive API responses with `no-store`.
- **Router.** A comptime table of `(method, pattern, role, handler)`; patterns are literal segments with at most two `{param}` segments; matching is a bounded loop with no allocation. Unknown paths under `/console/` return the shell so the interface module can route client-side; unknown paths under `/console/api/` return a JSON `404`.
- **Rate limits.** Token buckets keyed by client address for login (5 per minute) and by session for mutations (60 per minute); reads have per-session/global query, export and result-size budgets as well as the slot budget. Idle/read deadlines also cover slow response writers.

Rust port note (2026-10-15)
In the Rust kernel (`sibuna-serve`) heads are parsed by `sibuna_http::parse_request` with a stricter grammar, deadlines are kept in milliseconds, and a body cut short by the peer is an error. See the revision note.

10. Authentication and Authorization

- **Passwords** are hashed with Argon2id at the OWASP minimum recommended parameters (`t=2`, `m=19 MiB`, `p=1`) and stored as PHC strings; verification runs on the console's thread, never the data plane's, with a global single-verifier semaphore and bounded wait queue in addition to per-IP and per-account limits. Reserve the 19 MiB workspace and enforce supported PHC parameter maxima before verification; an IP limit alone cannot bound distributed login load.
- **Sessions** are 256-bit random tokens stored only as SHA-256 digests in `console_sessions` with an absolute lifetime (12 h) and an idle lifetime (30 min), delivered in an `HttpOnly; SameSite=Strict; Path=/console` cookie, `Secure` when behind a proxy. A session records the client address and User-Agent for audit; binding is an explicit console policy independent of data-plane proof tokens. Role changes, disablement and password resets revoke sessions and applicable tokens through an authorization revision. Privileged actions fail closed when current authorization cannot be established from the authoritative store.
- **Roles** form the order `viewer < operator < administrator`. Viewers read; operators edit policy, reputation, and bans; administrators manage users, tokens, GeoIP, retention, and settings. Every route declares its minimum role in the router table.
- **Cross-site request forgery** is prevented by the strict cookie plus a session-bound synchronizer token: the interface module receives a CSRF token at login and sends it in `X-Console-CSRF` on every mutation; the WebSocket upgrade is accepted only when `Origin` matches the console's configured canonical origin (scheme, host and port), not the untrusted Host header. Cookie-authenticated mutations require the token and same-origin checks; bearer-only API calls do not require a CSRF cookie. WebSocket commands are subscriptions only, with role/expiry/revocation rechecked during the stream.
- **Two-factor authentication** is optional per user and required for administrators when the console is bound off loopback: time-based one-time passwords (RFC 6238, HMAC-SHA1 from the standard library) enrolled through a QR code rendered by the interface module, with ten single-use recovery codes stored as digests. Encrypt the TOTP seed under a separately provisioned console key; atomically consume recovery codes and accepted TOTP time steps to prevent replay across nodes. Enrollment and recovery endpoints are rate limited. Seed envelopes use the standard-library XChaCha20-Poly1305 construction with a fresh 192-bit random nonce, binding the envelope version, console key identifier and user id as associated data. Recovery values contain 128 random bits and their SHA-256 digests are domain-separated and user-bound. Six-digit TOTP accepts at most one 30-second step of skew; the authoritative transaction consumes the newest matching step and refuses any previously consumed or older step. This is Phase 1 for any off-loopback release.
- **API tokens** for automation are opaque 256-bit values with a printable id, a role, and an optional expiry, presented as `Authorization: Bearer`; they are hashed like sessions.

- **Audit.** Every mutation writes one `console_audit` row (actor, role, action, subject, before and after summaries, address) in the same transaction as a database change. Redact passwords, token values, TOTP seeds, cookies and webhook secrets. Local effects use the intent/completion protocol above; exports and authentication outcomes also emit audit events.
- **Bootstrap.** `init-admin` atomically creates the first administrator with `must_change=true` and an expiring one-time password digest. Before initialization, HTTP serves only a "run init-admin locally" notice. A must-change account can only change its password and enroll required TOTP; consume the bootstrap credential and rotate the session atomically.

11. The Telemetry Pipeline

The pipeline combines existing counters and persisted incidents with proposed bounded instrumentation. "Exact" below means exact for the instrumented scope, not every connection.

11.1. The sampler

At 4 Hz the sampler reads `Metrics` using monotonic atomic loads; it sums four deltas into one second bucket and keeps 3,600 buckets. Loads are not a simultaneous snapshot. Persist minute deltas with node id, boot id, coverage and completeness. Use monotonic time for rates and UTC minute labels; a restart resets the baseline, never unsigned-subtracts the old process's counters. CPU usage is delta CPU seconds / delta wall seconds, not a sum of RSS. RSS is a gauge with last/max aggregation. Upsert partial minutes idempotently by boot id. Schema version 37 carries these gauges in the minute payload (format SBM2, version-36 rows stay readable): the console tick samples process CPU time and resident memory once per second, the open minute keeps the last and peak resident size and the CPU time consumed within it, and the live snapshot publishes resident size and CPU per mille of one core over the last second for the Nodes page and peer telemetry. Current resident size comes from the Linux process status; other platforms record the peak only and show the level as not recorded.

Current `requests` includes internal routes; `banned` counts requests rejected by the local ban table, not distinct banned addresses. `denied`, `challenged`, `allowed`, `rate_limited` and verification counters describe different branches; issued/accepted are separate requests, and malformed submissions may not increment `solutions_rejected`. Never stack them as an exhaustive partition. The console external-request outcome counter family assigns exactly one outcome (admitted, challenged, denied, banned, rate-limited, other) per external request. Here external means a successfully parsed request head outside `/__sibuna/`; incomplete external bodies count as other. Unparseable heads and pre-admission connection rejections cannot be classified by route and remain separate transport observations. Each selected outcome is recorded before attempting response delivery, so it does not prove receipt. Origin 4xx/5xx counts require response instrumentation; upstream errors are not their proxy. Distinct active bans are not derivable from the `banned` counter. The console tick reads the dynamic ban table once per second and publishes `active_bans`, the count of occupied, unexpired slots of that hashed table, as a gauge on the statistics snapshot; combined dashboards sum it over contributing nodes and withhold it when any contributor lacks the gauge. The same tick publishes `cluster_health`, this console's probe view of configured peers plus itself (healthy, degraded, down, unprobed), so a partial cluster is labelled rather than counted as healthy zeros. Both are levels, not rates: their tiles carry a sixty-second sparkline of observed snapshots and an explicitly unavailable day deviation.

11.2. The incident tap

The storage thread alone drains the existing 512-slot MPSC incident ring, up to 32 records per 500 ms tick: approximately 64 records/s before commit costs, with loss on overflow. A feeder polls committed rows using a separate sequence cursor *per issuer node*; a single maximum id would skip later records from lower-numbered nodes. Capture a cursor watermark with each snapshot, then send later rows. Bound pagination, report missing retention history, queue loss and replica staleness. Delivery includes queue drain, commit, feeder poll and 1 Hz fan-out; it is not bounded to one second during backlog or lost quorum.

Current rows retain node, IP, User-Agent (200 bytes), method (8), path (512), category (32), payload (512), campaign and timestamp. The payload is the query if present, otherwise body; it is not necessarily the matched substring. There is no full request/response capture, JA4, WEIGH decomposition, WAF numeric score, matched offset or rule version. Console-enabled capture now adds a version-1 metadata sidecar:

selected firewall status, query/body byte lengths and capture truncation flags. Query/body values and headers are omitted from this evidence view; selected status does not establish delivery. Historical rows have no sidecar. Richer evidence is opt-in: `--console-capture-heads` stores, in the incident's own transaction (schema versions 39 and 40), the request head redacted before capture and, for audited admissions in reverse-proxy mode, the origin response head (an accepted WebSocket handshake included). Redaction is an allowlist: only the values of Host, User-Agent, Accept, Accept-Encoding, Accept-Language, Content-Type, Content-Length, Content-Encoding, Cache-Control, Origin, Referer, Location, Connection, Upgrade, Sec-WebSocket-Version, Server, Date, Retry-After and X-Forwarded-Proto are kept; every other header keeps only its name, credential names (Cookie, Authorization and the like) lose their value even when listed, URL-bearing values lose userinfo, query values and fragments, and every query value reads "[redacted]". `--console-capture-header <name>` (repeatable, at most 16 token names of at most 64 bytes, deduplicated, rejected without the capture flag) adds names to the kept list. Bounds are 2 KiB and 1 KiB; the whole validated head is redacted first and truncation is flagged on the redacted copy, so a long credential never costs the bound. Findings held back for the origin head are recorded exactly once on every exit: a challenge, denial or rate limit records them with response state *local*, a relay that never produced a head with *unavailable*, a captured head with *captured*, and forward-auth mode with *unobserved*; rows written before version 40 read *unknown*, never local. Heads travel hex-encoded so the Events page renders them under UTF-8 or Latin-1, states the response condition, copies a cURL command through the host clipboard (with a selectable fallback), and refuses to build a command when the request line or Host is incomplete. The command uses `--globoff`, omits credential placeholders, framing and hop-by-hop headers, and names its redactions, the uncaptured body and an assumed scheme. Without the flag every incident reports its heads as not recorded. Show unavailable fields as "not recorded"; never reconstruct a raw request as if captured. Campaign similarity is the current 64-dimensional embedding/cosine heuristic (threshold 0.35), not attribution or proof of a common attacker. A denied request has no origin response.

11.3. The challenge funnel

Existing Prometheus counters expose issued, accepted and aggregate verification rejection. Console-owned counters now add submitted, malformed and exhaustive per-cause rejections at the verification endpoint. Window totals are a flow summary, not a cohort conversion rate: retries, abandonment and solutions crossing windows break that interpretation. Per-address records and adaptive-difficulty histories have their own bounded instrumentation: schema version 38 retains `console_challenge_records` (one row per issued, accepted or rejected challenge, drained from a 4,096-slot data-plane queue whose losses are counted and shown) and `console_challenge_difficulty` (one row per observed change of the adaptive bump, with the smoothed issue rate), both pruned at seven days. The fallback share remains unrecorded. Schema version 36 retains `console_challenge_minutes`: the console collector attributes per-tick deltas of the boot-local counters to the minute they end in, keeps at most eight active parameter partitions per minute (further partitions are counted as dropped), seals the minute on the roll and journals it exactly as traffic minutes are, including partial snapshots every five seconds and pruning under `retention.minutes`. The Challenges page sums a one-hour, one-day or seven-day window on the storage owner in bounded scans and shows recorded and complete minute counts beside the totals, so unrecorded minutes read as coverage, never as zero. Rule-hit totals likewise need fixed-capacity counters keyed by rule id and applied revision; incident counts cannot supply exact allow/WEIGH hits. Distinguish category findings from the one final outcome per request.

Accept optional `elapsed_ms` and solver metadata in the existing data-plane verify request; the interstitial now sends them. Measure solver time before verification, validate finite nonnegative bounds, and record only accepted solutions. Client timing is untrusted telemetry, never an admission or difficulty input. Use 16 buckets: [0,1) ms, powers-of-two intervals [1,2) through [8192,16384), and [16384,+infinity), with separate missing/invalid counts. Partition by algorithm and bounded parameter bins. Hashcash has expected trial count 2^b for b work bits; PoSW depth d requires $2^{d+1} - 1$ labels in this implementation. Do not label PoSW depth as a Hashcash security/work-bit equivalent or predict device solve time without calibration. Server response time and client solve time are different metrics.

11.4. Traffic sampling and top-k rankings

Use a per-connection PRNG with independently initialized state to select external requests with probability $p = 1/64$ by default. This avoids the periodic bias of every 64th request. Copy at most 256 bytes of explicitly

sized fields (including client IP, truncation flags, method/path prefix, client-family labels, Referer host and outcome/origin status) into one preallocated bounded MPSC queue drained by the console. Connection threads, not acceptor workers, are producers; one shared queue of 4,096 slots costs 1 MiB for records, plus queue metadata. A full queue drops and counts the sample; producer contention may require retries, so no single-CAS cost guarantee is claimed. Unsampled requests still pay the sampling test. Disable production when the console sampler is absent. Resolve country off the request path.

For N retained samples and $m = 256$ Space-Saving counters, every key with frequency greater than N/m is retained, and a tracked estimate obeys $\hat{f} - e \leq f \leq \hat{f}$ with $e \leq N/m$. This guarantees heavy-hitter inclusion, not exact counts or exact top-k order. Persist all 256 counters, their errors, N, sampling probability, losses and covered interval per kind; use a tested merge procedure for cross-minute/node queries. Saving only twenty local winners can lose a global winner. Counts scaled by $1/p$ are sampling estimates; queue loss, key truncation and sketch error remain visible. Use exact small sampled histograms for countries and response classes instead of a top-k sketch. Each sample also carries the referring host (a 24-byte host prefix, never a path or query) and the status selected for the client or observed from the origin; an admitted request offers its sample once the origin status is known. Referring hosts use a second Space-Saving sketch under the same bound, while operating system, browser and status are exact histograms over bounded label sets from a deterministic User-Agent classifier (`client_family`). The SBR2 archive retains all of them beside paths; SBR1 archives stay readable and report those dimensions as absent, never as zero. Country history must survive minute folding. Visitors, page views and a complete traffic log are not inferred.

11.5. Data-plane changes this record requests

The proposed work exceeds three atomic additions: outcome/response metrics, rejection and client-timing histograms, the sample queue, bounded challenge events and richer incidents, control commands, and new policy snapshot fields all require implementation and impact tests. Current WAF configuration is a global boolean. Add per-category disabled/audit/enforce modes inside inspection; audit records a finding and *continues* evaluation, so another enforcing category, reputation denial or later rule can still block. Disabled categories skip detection. New per-rule limits and page templates require loader and request-path changes; a database schema alone does not activate them. Validate the immutable snapshot before commit and publish only from storage/control code; failed rebuilds retain the prior snapshot and surface an error.

11.6. Cluster aggregation

Minute history sums disjoint node/boot intervals; exclude overlapping live seconds already covered by persisted minutes. Report node coverage, clock skew, reset/gap and stale values. Replicated minute rows and configured probes provide historical coverage and health. Direct TLS peer snapshots now supply each node's local statistics, tagged by node, boot, sequence and observation interval. Received totals are never forwarded as a node's own contribution. The dashboard composes configured sources and permits individual-node selection. Only nodes running telemetry contribute; label a partial cluster rather than treating missing members as zero. Applied policy revision is a per-node acknowledgment, not evidence inferred from a committed row. Client dashboards do not connect directly to data-plane listeners.

12. The Real-Time Protocol

One WebSocket per browser tab at `/console/ws`, opened after login. Frames are JSON text.

Direction	Operation	Fields and behavior
Client to server	`sub`	`topic`, `args`: subscribe; snapshot precedes deltas.
Client to server	`unsub`	`topic`: stop a subscription.
Client to server	`filter`	`topic`, `args`: replace filter and start a new epoch.
Client to server	`ping`	Application heartbeat, distinct from a transport ping.
Server to client	Snapshot	`topic`, `epoch`, `seq`, `snapshot`, `data`: full bounded state, chunked if necessary.
Server to client	Delta	`topic`, `epoch`, `seq`, `data`: coalesced updates; events carry bounded summaries.

Direction	Operation	Fields and behavior
Server to client	Gap	`topic`, `epoch`, `dropped`: resubscribe for a new snapshot; never apply deltas across the gap.
Server to client	Unauthorized	`error`: close the subscription and return to sign-in.

Example subscription and initial unavailable snapshot (separate JSON messages). `epoch` changes on reconnect, filter replacement or server restart. The initial view becomes visible only after `snapshot_end`; subsequent patches replace unavailable state with observations. Historical time windows use the bounded HTTP timeline/minute APIs, alongside the live stream.

```
{"op":"sub","topic":"stats","args":{}}
{"op":"snapshot_begin","topic":"stats",
 "epoch":"aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa:1","seq":0,
 "snapshot":true,"watermark":0,"parts":1}
{"op":"snapshot_chunk","topic":"stats",
 "epoch":"aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa:1","seq":1,
 "snapshot":true,"watermark":0,"part":0,"parts":1,
 "data":"{\"available\":false}"}
{"op":"snapshot_end","topic":"stats",
 "epoch":"aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa:1","seq":2,
 "snapshot":true,"watermark":0}
```

The hub keeps one bounded ring per topic (1,024 entries of at most 2 KB) and a cursor per subscriber. Publication uses preallocated storage and never waits on network writes; a slow consumer sees a `dropped` count rather than growing memory. The ring and subscriber outbox are separate bounded owners. Fan-out runs on the hub thread, which writes into each connection's bounded send queue; a full queue invalidates the affected topic, removes its queued frames and reserves a gap notice before surviving data. That topic resumes only with a new subscription epoch, so a stalled tab cannot complete a broken snapshot or grow an unbounded backlog. Subscribers are capped at 64 per console; the 65th receives a `503` at upgrade. Reserve separate HTTP/control capacity so 64 long-lived sockets cannot prevent login or API requests. Sequence numbers are per subscription with an epoch; filters start a new epoch/snapshot. A 2 KiB ring entry carries a bounded event summary, not a 64-record full-payload batch. Chunk snapshots with explicit begin/end watermarks; bound reassembly and resynchronize after a gap. Reconnect with jittered backoff, show stale age and keep the last good view.

Listing 1 One browser session: login, upgrade, subscribe, live deltas, a mutation, and the policy rebuild it causes on every node. Storage arrows represent mailbox requests; password verification runs between the user read and session write, outside a storage transaction. Solid arrows are requests; dashed arrows are responses and asynchronous effects.



13. Data Model

All console tables live in the same Zaxonlite database as SID 0005 and replicate with it. Migrations are numbered and version-gated in `schema.zig`. The authoritative writer serializes each migration and schema-version update; followers wait for application before serving compatible routes. Never run concurrent startup DDL independently on every member. All tables below are proposed. Bound row/result sizes and use typed SQL operations with parameter binding where supported (otherwise audited literal escaping), never client-supplied SQL. Console object IDs must be globally unique (random 128-bit ids or node-scoped sequences); foreign keys and uniqueness constraints are required.

Table	Columns and purpose
`console_users`	`id`, `name` (unique), `role`, `password_phc`, `must_change`, `disabled`, `auth_revision`, `last_login`, `totp_ciphertext`, `totp_key_id`, `totp_last_step`, `created_at`, `updated_at`
`console_sessions`	`digest` (primary), `user_id`, `role`, `client_ip`, `user_agent_hash`, `csrf`, `issued_at`, `last_seen`, `expires_at`, `auth_revision`, `kind` (`browser` or `kiosk`); expired rows are purged by retention
`console_kiosk_grants`	`digest` (primary; SHA-256 of the one-time code), `user_id`, `revision`, `label`, `created_at`, `use_by` (ten minutes), `expires` (twelve hours), `consumed_at`; at most 64 outstanding; audit `kiosk.grant` and `kiosk.exchange` never carry the code; retention removes consumed and unusable rows
`console_tokens`	`id` (printable), `digest`, `label`, `role`, `scopes`, `auth_revision`, `created_by`, `created_at`, `expires_at`, `disabled`
`console_audit`	`id`, `at`, `actor`, `role`, `action`, `subject`, `before`, `after`, `client_ip`; append-only
`console_settings`	`key` (primary), `value` ($\leq$ 1 KiB, never a secret), `revision`, `updated_at`, `updated_by`; the denial-spike minimum/factor and bounded retention days; every change is audited with its before and after value
`console_notifications`	`id`, `kind` (`webhook` or `syslog`), `label`, `target`, `target_host`, `secret_envelope` (sealed under the console key and bound to the target), `events` bitmask (denial spike, ban, node unhealthy, leader change), `cooldown_seconds`, `enabled`, `revision`, created/modified actor and time, last attempt, outcome and detail; at most eight rows; audit summaries carry kind, label, events, cooldown, enabled state, whether a secret is set and the host only
`console_notification_events`	`node`, `boot`, `sequence` (unique per node and boot), `event`, `raised_at`, `detail`, completion time; every node enqueues what it observed, at most 256 pending and 4,096 total rows; completed history expires after seven days. The legacy event-wide attempts column is no longer authoritative
`console_notification_deliveries`	One event/destination pair and pinned destination revision; pending/sending/delivered/failed/skipped state, at most three attempts, next due time, claim fence/expiry and redacted outcome. Destination edits invalidate queued work; parent completion and outcome audit commit with each transition
`console_job_leases`	`job` (`retention` or `notifier`), `node`, `boot`, `fence`, `expires`; one fenced singleton lease per job name
`console_pages`	`kind` (primary: `challenge`, `denied`, `rate_limited`, `banned`, `overloaded`), `html` ($\leq$ 16 KiB, validated before staging), `sha256`, `revision`, `updated_at`, `updated_by`; a one-row stage table commits the page, its audit record (`page.edit` or `page.reset` with digests and sizes only) and a policy-version bump together so the next tick rebuilds the snapshot
`ip_reputation` (added columns)	`source` (`console`, `console:country:XX`, or empty for data-plane rows), `note` ($\leq$ 128), `geo_generation` (the GeoIP generation digest a country block was computed from); one-row stage tables `console_policy_order_stage`, `console_reputation_stage`, `console_country_commit` and `console_policy_import_commit` commit each workflow with its history rows, audit record and an explicit policy-version bump; `console_country_stage` and `console_policy_import_stage` hold chunked prefixes and canonical documents for ten minutes

Table	Columns and purpose
`traffic_minutes`	`node_id`, `boot_id`, `minute` (epoch/60), coverage, completeness, counters from "The sampler", `rss_last_kib`, `rss_max_kib`, `cpu_delta_seconds`; primary key (`node_id`, `boot_id`, `minute`)
`challenge_minutes`	`node_id`, `boot_id`, `minute`, algorithm/parameter bin, submitted/issued/accepted, rejected by exhaustive cause, missing/invalid timing, coverage, `solve_ms_buckets` (16 integers)
`topk_minutes`	`node_id`, `boot_id`, `minute`, `kind`, `key`, estimate and error; all bounded sketch counters plus N, probability, losses and coverage metadata
`geoip_ranges`	`generation`, `start` (16-byte address as blob), `end`, `country` (ISO 3166-1 alpha-2); one row per range from the source CSV
`geoip_meta`	`generation`, `active`, `source`, `licence`, `published`, `loaded_at`, `ranges`, `sha256`
`console_nodes`	`node` (primary), `address` (the member's consensus endpoint, or `local`), `console_url` (the advertised console origin, rendered only as a plain-origin link), `version`, `boot`, `first_seen`, `last_seen`, `applied_revision`, `control_revision`, `applied_slot`, `decided_slot`, `draining`; each node writes only its own row from the storage owner: at start, every minute, and after every successfully applied policy rebuild

Additional migrations are required for `console_recovery_codes` (digest and consumed state), `console_policy_history` (revision and bounded documents for conflict-checked revert), `console_jobs` (import/notifier/retention leases with expiry, fencing token and progress), `console_node_commands` (target, operation id, expiry, desired state and acknowledgment), `country_minutes` (node/boot/minute/country/outcome, sample count, probability and coverage), and versioned incident/challenge evidence. Authentication-only changes must not trigger policy rebuilds. Coalesce session activity writes; specify replica-staleness handling for idle expiry. Audit is append-only to application users until explicit retention deletion; it is not cryptographically tamper-proof. Retention deletes associated FTS/vector rows in the same transaction and reports maintenance lag.

Existing tables are read, and two are written: `policies` (rule editor) and `ip_reputation` (ban and allow actions, GeoIP-derived blocks), using the existing row formats for currently supported operations. Dynamic rules sort by `(priority, name)` before file rules, within the larger WAF/reputation/rules evaluation order. Preflight the whole candidate snapshot (128 total rules, matcher limits, 8,192 trie nodes) before commit; use an expected revision to prevent lost updates. New modes, limits and templates require rebuild-path changes. Report committed and applied status separately, including per-node failures.

14. GeoIP

Country enrichment runs only off the request path. The first-party library `libs/geoip` (standard library only; never imported by the data plane) owns address normalization, row validation, the immutable sorted generation with binary-search lookup, the compact `SBGEOIP1` snapshot format and every provider fact. The default provider is the `user-country` dataset of ip-location-db: public domain under the PDDL 1.0 (no attribution), rebuilt daily from RIR delegated statistics, public BGP archives and RFC 8805 geofeeds, published as two uncompressed `start,end,country` CSV files with a SHA-256 file each. DB-IP IP to Country Lite remains selectable as a second provider: monthly, CC BY 4.0, one gzip archive, attribution shown wherever its data is displayed. MaxMind GeoLite2 is not offered; its licence requires an account and its CSV joins network blocks to location records. The generation digest is the SHA-256 of the source bytes in provider file order; per-file publisher digests are recorded and enforced when the provider publishes them, and an operator checksum pins the generation. A GitHub release download is followed through exactly one HTTPS redirect to an allowlisted asset host; any other hop fails. An optional `-Dgeoip-data=<snapshot>` build flag embeds a validated snapshot that serves lookups at revision 0 until the first durable import replaces it. Unknown, private, reserved and unmapped addresses stay in "Unknown" and never acquire an invented country; the transitionally reserved codes `AN` and `FX` that RIR-derived data still carries are accepted.

The loader bounds download/compressed and expanded sizes, row count, string lengths and transaction sizes. HTTPS and an operator/publisher checksum when available protect transfer; a locally computed

digest identifies a dataset but does not authenticate its publisher. Parse and validate address families, ordering, non-overlap and country codes, stage an immutable generation, and atomically switch its active id only after validation. Replicate bounded batches through the storage mailbox. Keep the previous generation until readers release it, with at most two in-memory generations and one bounded import in flight. Use sorted normalized 16-byte addresses with explicit IPv4 mapping semantics and binary search. Memory is `capacity` × `@sizeOf(Range)` per generation; neither range count, 10 MB, sub-microsecond lookup nor a one-minute import is an established result.

> **Rust port note (2026-10-15)**
> The Rust loader reserves nothing up front, so a generation takes 34 bytes per loaded range (16-byte first and last addresses and a 2-byte country code in three arrays) rather than its capacity times `@sizeOf(Range)`.

An operator may preview a country's ranges decomposed into exact CIDRs, with deduplication, expiry and overlap analysis. Existing reputation maps scores ≤ -50 to deny and ≥ 50 to allow; it does not load challenge verdicts. Country challenge requires explicit declarative challenge rules and their limits, or a separately specified extension. Reject an entire country action if the candidate engine would exceed 8,192 trie nodes or 128 total rules; never apply a truncated country. GeoIP updates do not silently change existing country policies: pin the generation and require a reviewed diff to refresh them.

14.1. Live earth globe on the landing page

The front-page focal panel is a real-time earth globe showing traffic by country whenever GeoIP is loaded. A pinned, attributed low-resolution world-boundary asset supplies geometry; country-centroid markers are representative positions, not measured client coordinates. Do not infer city-level locations or geographic destination coordinates from country-only data. Animate aggregate inbound arrows from observed countries to a clearly labelled, non-geographic Sibuna service hub until a node location is explicitly configured. These arrows illustrate the rolling sample window, not individual packets or invented country-to-country connections. Zig generates an orthographic SVG projection with a configurable center (λ_0, ϕ_0): $x = \cos\phi \sin(\lambda - \lambda_0)$, $y = \cos\phi_0 \sin\phi - \sin\phi_0 \cos\phi \cos(\lambda - \lambda_0)$, $z = \sin\phi_0 \sin\phi + \cos\phi_0 \cos\phi \cos(\lambda - \lambda_0)$. Draw only $z \geq 0$ and clip/split coastlines at the horizon and antimeridian; map to screen coordinates $(c_x + Rx, c_y - Ry)$. Displaying the rear hemisphere through the sphere is a bug. Preprocess geometry to a bounded vertex budget, simplifying before runtime.

Update country counts at 1 Hz over a rolling 60-second window via the `stats` subscription. Default to sampled traffic with coverage, sample probability, lost samples, unknown count, last update and node coverage visible; switching to persisted incidents explicitly labels that incomplete incident population. Use marker area proportional to count (radius grows with the square root of count, capped), and discrete intensity classes on country fills. A ranked country table next to the globe contains *all* hemispheres and offers keyboard selection to center the globe and open filtered events. Provide continuous rotation with a separate animation pause, Rotate left/right, reset, pause/live and a flat-map alternative. Manual country selection pauses automatic rotation for inspection. Hidden tabs suspend visual updates and resnapshot on return. A globe is one panel, not a replacement for totals.

Without GeoIP, keep the earth outline and show "GeoIP unavailable", Unknown totals and an administrator setup link; no synthetic country markers. With zero traffic say "No traffic in this window". On disconnection freeze the last good state and label its age; never animate stale traffic. Use accessible text/table equivalents; user-driven rotation honors reduced motion. The same globe component serves desktop, responsive and kiosk views.

The lightweight implementation caps animation at 24 frames per second and 16 visible arcs. Only the SVG globe region is replaced per frame; statistics retain their independent 1 Hz subscription cadence. Geometry and animation state remain in Zig, while the browser bridge supplies frame timestamps and the reduced-motion preference. Reduced motion disables automatic rotation and moving arrows. Curves use bounded quadratic paths with directional arrowheads. The inspiration is GitHub's globe; its connection endpoints come from actual pull-request location pairs, whereas Sibuna currently has country-only source observations and a logical service endpoint.

15. Cluster Management

The `nodes` page shows every member known from the replicated `console_nodes` table and from this console's probe configuration: id, consensus address, version, boot, the policy revision that node has applied against the committed revision, its log frontiers, and the health of its data-plane listener. Role, leader, ballot term and quorum availability come from a storage-owned snapshot the owner thread refreshes at most once per second: a single node reads its own status; a cluster member asks its own Zaxonlite endpoint over the local status RPC. Health is probed by each console over explicitly configured data-plane addresses given as `--console-probe <node-id>=<http://ip:port>` (numeric hosts only, never an address read from replicated data or a browser) with `GET /__sibuna/health` and `/__sibuna/metrics` every 5 seconds, bounded to 2 s per probe, on one console-owned thread. A member configured for probing but without a replicated row renders as unobserved with its counters unavailable, never zero. `--console-advertise <origin>` names the link peers show for this console. This lets a console show a member whose storage has failed but whose data plane still serves from its last snapshot, the failure mode SID 0005 documents.

Operations offered per node: drain (set a flag the node's accept loop reads, so it answers `503` to new connections while finishing current ones, for maintenance), clear local bans (a control command; a replicated reputation denial can still apply), and open that node's own console. Cluster-wide operations are edits of replicated tables and need no per-node action: a rule saved on any console is a `policies` row; a ban is an `ip_reputation` row; both require commit, replica application and the next successful storage rebuild. Book benchmark results are workload-specific and do not establish a 100 ms bound at the default 500 ms polling interval. The page also shows the two facts an operator must know from SID 0005: challenge verification is issuer-bound (sticky routing is needed), and rate limits are per node.

16. The Interface Module

The interface follows the zenfmt approach: a `wasm32-freestanding` Zig module owns every page, all interface state, and every fragment of markup; the glue owns the browser. The glue loads the module, opens the WebSocket only after authentication, forwards browser events and WebSocket frames into the module as length-prefixed JSON, and executes the returned command list: `patch` (replace an element's inner HTML), `attr`, `class`, `focus`, `navigate` (push state), `fetch` (issue an API request the module described and post the result back), `ws` (send a frame), `download`, `theme`. No markup, route, or form logic lives in JavaScript, so the golden tests compile the same module natively and assert rendered HTML strings.

- **Rendering.** Pages render into a fixed 512 KB output buffer with a bounded HTML writer that escapes by construction. First-party HTML snippets use `{{ field }}` placeholders expanded at build time by the native/Wasm-compatible `libs/html` renderer; Zig supplies runtime values. Text is always escaped, unknown fields fail compilation, and templates cannot request raw output. Snippets are capped at 32 KiB and 128 placeholders; caller-owned output remains bounded. Conditions, bounded loops and snippet composition stay in Zig. This is separate from the constrained operator-editable data-plane page templates. A page re-renders only the panels whose inputs changed (each panel is a function of a slice of state with an explicit version), so a one-second stats delta patches four tiles and one chart, not the document.
- **Charts** are inline SVG produced by `charts.zig`: an external-outcome timeline (admitted, challenged, denied, banned, rate-limited and other), sparklines, horizontal bars, a donut, a histogram, and the orthographic earth globe and country table generated from the committed `world-110m.bin` (bounded longitude/latitude polygon vertices keyed by ISO code, projected to SVG at runtime; a flat-map SVG alone cannot supply rotating globe geometry). Decimate long timelines to the visible pixel width and enforce the output bound; output size depends on series and coordinate encoding, not just point count; no charting library is loaded, and no canvas is used, so the charts print, zoom, and are accompanied by titles and equivalent data tables; SVG titles alone do not establish accessibility.
- **Components.** daisyUI 5 supplies the primitives (`btn`, `card`, `table`, `drawer`, `badge`, `tabs`, `toast`, `modal`, `stat`). First-party `sb-*` components compose them with fixed markup and are the only elements the render functions emit: `sb-shell`, `sb-tile`, `sb-timeline`, `sb-table` (virtualised rows, sortable, with a filter bar), `sb-drawer` (event detail), `sb-form` (schema-driven, with validation messages in the daemon's Elm-style diagnostic voice), `sb-flag`, `sb-node-card`, `sb-diff`.

- **Visual system.** One daisyUI theme, `sibuna`, defined in `tailwind.css` from the tokens of the Elegance subsection (accent, four decision colours, five neutral surfaces, the type scale, the 8-pixel unit) with `sibuna-light` and `sibuna-dark` variants selected by `data-theme`, following the system preference by default and remembered per browser, together with the density preference. The `sb-*` components consume only these tokens; a component that needs a new colour is a design change, reviewed as one.
- **Charts obey the rules.** `charts.zig` has one palette (the decision colours and the accent), draws deviation markers and sparklines as first-class marks, keeps axes and positions stable across updates, and uses no animation on data updates (R6, R8 to R11).
- **Budget.** The module is compiled at `ReleaseSmall`, with a 640 KiB artifact review warning and 768 KiB uncompressed ceiling (raised from 448 KiB and 512 KiB on 2026-09-11; see "Interface budget review"). These project guardrails cover the complete console; they are not WebAssembly limits or substitutes for browser performance acceptance. The ceiling is a project allocation, not a WebAssembly standard. Correctness, accessibility and cohesive modules take precedence over recovering a few bytes through complex encoding. Crossing the warning requires a dependency and browser-timing review; changing the ceiling requires evidence. At 4 Mbit/s, 768 KiB alone takes about 1.57 seconds before latency and other assets, an arithmetic planning assumption rather than a measured load time. Linear memory remains 4 MiB initial and explicit maximum, with bounded retained history and a bump arena reset after each event.

Rust port note (2026-10-15)

The Rust module renders into an owned, reused string bounded at 512 KiB, parses each event into a tree bounded by the event size instead of a bump arena, erases freed memory in its allocator, and declares a 16 MiB maximum linear memory instead of a fixed 4 MiB. See the revision note.

16.1. Pages

All panels are conditional on the instrumentation in "Data-plane changes this record requests". Missing fields stay explicitly unavailable; none of the wireframe examples establishes current capture support.

Page	Panels
Setup and login	First-run password change; login form with the optional one-time code; session expiry notices.
Statistics / Traffic	Period selector (live boot totals, 1 h, 24 h, 7 d, 90 d) and node selector; tiles (requests, admitted, challenged, denied, banned addresses, origin 4xx and 5xx with rates, nodes healthy); live timeline of disjoint external outcomes; queries-per-second, request-status and blocking-status sparklines; live orthographic earth globe with a ranked country table, 60-second sampled traffic window, manual rotation, pause and flat-map fallback ("Live earth globe on the landing page"); top-five panels: client operating systems, browsers, response status, referring hosts, popular paths, all marked as sampled.
Statistics / Security	Tiles per module (inspection, reputation, rate limiting, challenges, bans, honeypot); a trend chart per module with its top source addresses; the live event feed; attack-category donut; attacked paths; rule hits.
Kiosk	The traffic and security panels in a full-screen, read-only, optionally auto-cycling layout (off with reduced motion) for a wall display. An operator or administrator mints a one-time code (`POST /console/api/kiosk/token`, shown once, usable for ten minutes); the display pastes it into a second form on the sign-in page and receives a viewer cookie session scoped to statistics that expires with the grant (twelve hours) and with the granting user's revision. Codes and sessions never travel in URLs, fragments or local storage.
Attack events	Grouped view (source address, country, node, attack count, first and last seen) and raw view (action, URL, category, rule, address, time, detail); filter bar (node, category, rule, address, country, path, period); export; detail modal (category chip, URL, address with country and "ban", "allow", "add to group", "address info" actions, JA4 only after trusted-ingress capture is implemented, payload location and decoded value with the

Page	Panels
	matched structure highlighted, rule and score, campaign and its members, similar incidents, request and response heads with charset selection, “copy as cURL”).
Challenges	Funnel (issued, submitted, accepted, rejected by cause); solve-time histogram by algorithm and difficulty; adaptive-difficulty bump timeline; JavaScript-fallback share; per-address records (issued, accepted, rejected, cause, duration, start); per-rule challenge parameters.
Policy	Rules table with drag ordering, enable toggle, type (allow, deny, challenge, weigh), name, match summary, hits today, creator, updated; rule editor (form and JSON); pattern tester; import and export; inspection mode matrix per category (disabled, audit, enforce); limits (rate, window, ban seconds); IP groups (reputation prefixes with score, expiry, trigger, source, hits); GeoIP block builder.
Nodes	Member cards with surface, upstream, listener, role, health, version, requests and blocks today, sparklines; per-node drain and clear-bans; replication lag; the sticky-routing and local-limit notices.
GeoIP	Source, licence, published date, ranges loaded, last update, update button, attribution text.
Settings	Users (role, two-factor state, last login); API tokens; pages (challenge, denied, rate limited, banned, overloaded templates with preview); retention (minutes, incidents, audit, samples); notifications (webhooks, syslog; events: denial spike, ban, node unhealthy, leader change); about (version, node id, build, binding and proxy facts).
Audit	Append-only log with actor, action, subject, before and after, filterable and exportable.

17. Wireframes

These drawings specify every route and key workflow; illustrative values are not benchmark results. Setup/sign-in are authentication-only: no globe geometry is fetched or decoded, no GeoIP query runs and no telemetry WebSocket opens until successful login (and required password change/TOTP). Then navigate to Statistics / Traffic and load the dashboard assets. Sign-out closes streams, clears retained telemetry and returns to the authentication shell. Dashboard globe controls select Traffic or Attacks; the latter shows recorded security incidents with loss/coverage warnings, not an exhaustive attack count.

The drawings fix layout and information density, not visual style; the visual system of the Elegance subsection supplies the style. Every panel named here maps to one `sb-*` component and one render function, and every page is laid out to pass the audit of the principle audit: tiles first, trends second, tables third, detail on the right or in a modal, and the way back in the same place on every page.

The drawings below are ASCII redrawings of the original Typst wireframes. In them, `>` marks the active sidebar page, `v` a drop-down, `(ext)` a link that opens elsewhere, `[...]` a button or input, `* Live` the live indicator, and `#` a bar; `o` and `x` on a globe mark traffic (blue) and attack (red) countries.

Listing 2 The shell: top bar with cluster status and the account menu, a fixed sidebar of the eight pages, and the page body. Below 1,024 px navigation becomes a labelled menu drawer.

```
+-------------------------------------------------------------------------------+
| SIBUNA                          cluster: edge-eu - 3/3 healthy - admin v - (theme) |
+--------------+----------------------------------------------------------------+
|>Statistics   |                                                                |
| Attack events| +------------------------------------------------------------+|
| Challenges   | | page body                                                  ||
| Policy       | |                                                            ||
| Nodes        | |                                                            ||
| GeoIP        | |                                                            ||
| Settings     | |                                                            ||
| Audit        | |                                                            ||
|              | +------------------------------------------------------------+|
|              |                                                                |
+--------------+----------------------------------------------------------------+
```

Listing 3 Login and first-run setup. The setup variant replaces the password field with the one-time password and a new-password pair, and forces a change.

```
                      +--------------------------------------+
                      |             SIBUNA CONSOLE           |
                      |                                      |
                      | +----------------------------------+ |
                      | | user name                        | |
                      | +----------------------------------+ |
                      | +----------------------------------+ |
                      | | password                         | |
                      | +----------------------------------+ |
                      | [             Sign in              ] |
                      |                                      |
                      +--------------------------------------+

              Authentication required - no telemetry before sign-in
         Five attempts per minute per address - sessions expire after 30 idle minutes
```

Listing 4 The signed-in landing page: Traffic overview with a live country-level earth globe, ranked countries across both hemispheres, traffic totals and timeline. Values and geography are illustrative; sampling, Unknown coverage and freshness are explicit.

```
+--------------+-------------------------------------------------------------------------+
| SIBUNA       | edge-eu / All nodes / Statistics / Traffic            [Light / Dark]  |
| CONSOLE      | 3 of 3 nodes reporting - last update 1 s ago    [admin v - Sign out]  |
|              |-------------------------------------------------------------------------|
|>Statistics   | TRAFFIC OVERVIEW               [All nodes v] [Last 24 h v] [* Live]  |
| Attack events| External requests - UTC - illustrative data after successful login    |
| Challenges   | [Traffic] [Security]                                  [Kiosk (ext)] |
| Policy       | +--------------------+ +--------------------+ +--------------------+  |
| Nodes        | | Requests - 24 h    | | Admitted           | | Challenged         |  |
| GeoIP        | | 1.28 M             | | 1.19 M             | | 64 k               |  |
| Settings     | | +8.2% vs prior day | | +7.1% vs prior day | | +3.4% vs prior day |  |
| Audit        | +--------------------+ +--------------------+ +--------------------+  |
|              | +--------------------+ +--------------------+ +--------------------+  |
|              | | Denied             | | Banned /           | | Reporting nodes    |  |
|              | | 21 k               | | rate-limited       | | 3 / 3              |  |
|              | | -2.1% vs prior day | | 5 k                | | Coverage complete  |  |
|              | +--------------------+ | Separate outcomes  | +--------------------+  |
|              |                        +--------------------+                         |
|              | +-----------------------------------------+ +----------------------+|
|              | | LIVE EARTH GLOBE     [Traffic] [Attacks]| | TRAFFIC TIMELINE     ||
|              | | Last 60 s - GeoIP by DB-IP - countries,  | | 2,140 req/s now -    ||
|              | | not precise locations                    | | external outcomes    ||
|              | |                                          | |                      ||
|              | |                   Country     Est. req.  | | 2 k ................ ||
|              | |     .-~~~~~~-.    United States  38.4 k  | |      a  aa    aa  a  ||
|              | |   .' o ox    '.   #############        | |     a aa  aaa  aa a  ||
|              | |  /    .      x \  Germany        25.6 k  | | 1 k ................ ||
|              | | |   .  o        | #########            | |                      ||
|              | | | o      .      | India          19.2 k  | |     cc ccc  ccc cc c ||
|              | |  \      o     /  ######               | | 0   ddddddddddddddddd ||
|              | |   '.         .'  Brazil         12.8 k  | |     00:00  24:00 UTC ||
|              | |     '-~~~~~~-'   ####                 | |                      ||
|              | |                  Japan           6.4 k  | | a Admitted -         ||
|              | |                  ##                     | | c Challenged -       ||
|              | | o traffic (blue)  x attacks (red)       | | d Denied             ||
|              | |                                         | | Banned / rate-       ||
|              | | [<- Rotate] [Rotate ->] [Reset]         | | limited / other in   ||
|              | | [Flat map] [Pause]          Unknown 4%  | | detail (ext)         ||
|              | +-----------------------------------------+ +----------------------+|
|              | +--------------------+ +--------------------+ +--------------------+  |
|              | | Origin status      | | Popular paths      | | Client families    |  |
|              | | (sampled)          | | (sampled)          | | (sampled)          |  |
|              | | 2xx 92%  4xx 5%    | | / 42%  /api 31%    | | Chrome 58%         |  |
|              | | 5xx 3%             | | /login 12%         | | Safari 22%         |  |
| node 1 - Edge| +--------------------+ +--------------------+ +--------------------+  |
| v0.1.0 -     | Geo sample p = 1/64 - loss 0 - known country 96% - blue: traffic /    |
|  proposed UI | red: attacks - table includes hidden hemisphere                       |
| Operator     | Wireframe only - illustrative traffic and simplified geography -      |
```

```
|  guide (ext) | example data                                                          |
+--------------+-----------------------------------------------------------------------+
```

Listing 5 Statistics / Security: one tile and one trend per module, the live event feed, and the rankings that answer "what was attacked".

```
+-------------------------------------------------------------------------------------+
| SIBUNA                           cluster: edge-eu - 3/3 healthy - admin v - (theme) |
+--------------+----------------------------------------------------------------------+
|>Statistics   | STATISTICS                   [TRAFFIC - SECURITY - KIOSK (ext)]      |
| Attack events|                                                                      |
| Challenges   | +------------+ +------------+ +------------+ +------------+          |
| Policy       | | 21 k       | | 1,204      | | 3,318      | | 64 k       |          |
| Nodes        | | inspection | | reputation | | rate       | | challenges |          |
| GeoIP        | | denials    | | hits       | | limited    | |            |          |
| Settings     | +------------+ +------------+ +------------+ +------------+          |
| Audit        | +------------+ +------------+                                       |
|              | | 312        | | 41         |                                       |
|              | | bans       | | honeypot   |                                       |
|              | |            | |            |                                       |
|              | +------------+ +------------+                                       |
|              | +--------------------------------+ +---------------------------------+|
|              | | inspection trend - top         | | REAL-TIME EVENTS                ||
|              | | addresses                      | |                                 ||
|              | |                                | | [inspection] sqli - node 2 -    ||
|              | |      _/\  /\_  address    n    | |   198.51.100.7         12:41:07 ||
|              | |  /\_/   \/   \ --------- --    | | [honeypot] ban - node 1 -       ||
|              | | /              --------- --    | |   203.0.113.9          12:41:02 ||
|              | |                --------- --    | | [rate limit] 429 - node 3 -     ||
|              | +--------------------------------+ |   192.0.2.44           12:40:58 ||
|              | +--------------------------------+ | [challenge] rejected - double   ||
|              | | rate limiting trend - top      | |   spend                12:40:51 ||
|              | | addresses                      | | [reputation] deny prefix        ||
|              | |                                | |   2001:db8::/32        12:40:40 ||
|              | |      _/\  /\_  address    n    | | [inspection] xss - node 1 -     ||
|              | |  /\_/   \/   \ --------- --    | |   198.51.100.7         12:40:33 ||
|              | | /              --------- --    | +---------------------------------+|
|              | |                --------- --    | +---------------------------------+|
|              | +--------------------------------+ | ATTACK CATEGORIES               ||
|              | +--------------------------------+ |                                 ||
|              | | challenges trend - failed      | |   .-=-.   sqli 48%              ||
|              | | solvers                        | |  /     \  xss 22%               ||
|              | |                                | |  \     /  traversal 17%         ||
|              | |      _/\  /\_  address    n    | |   '-=-'   rce 9%                ||
|              | |  /\_/   \/   \ --------- --    | |           honeypot 4%           ||
|              | | /              --------- --    | +---------------------------------+|
|              | |                --------- --    | +---------------------------------+|
|              | +--------------------------------+ | ATTACKED PATHS - RULE HITS      ||
|              |                                    |                                 ||
|              |                                    | /search      ###########        ||
|              |                                    | /login       ######             ||
|              |                                    | /.git/config #####              ||
|              |                                    | /wp-admin    ###                ||
|              |                                    | /api/v1      ##                 ||
|              |                                    +---------------------------------+|
+--------------+-----------------------------------------------------------------------+
```

Listing 6 Attack events with the detail modal open over the raw view. New rows wait behind a "Show new events" control while the reader is interacting; the modal keeps the layout operators know and adds available rule evidence, the campaign, and the nearest incidents. Raw-head capture shown below is a proposed redacted extension, not current stored evidence.

```
+-------------------------------------------------------------------------------------+
| SIBUNA                           cluster: edge-eu - 3/3 healthy - admin v - (theme) |
+--------------+----------------------------------------------------------------------+
| Statistics   | ATTACK EVENTS                [BY SOURCE - RAW]                       |
|>Attack events| [node v] [category v] [rule v] [address] [country v] [path]          |
| Challenges   | [period v] [* live] [export]                                         |
| Policy       | action | URL          | category | rule   | address - country | time >|
| Nodes        | ------ | ------------ | -------- | ------ | ----------------- | ---- >|
| GeoIP        | ------ | ------------ | -------- | ------ | ----------------- | ---- >|
| Settings     |  +-------------------------------------------------------------+ |
```

```
| Audit        |  | [waf:sqli] GET /search?q=%27%20OR%201%3D1-- - node 2 -          | |
|              |  |            2026-09-08 12:41:07                                 | |
|              |  |                                                                | |
|              |  | address       198.51.100.7 - Unknown (documentation IP) -      | |
|              |  |               [Ban 24 h] [Allow]                               | |
|              |  | JA4 (from     Not recorded - requires trusted-ingress          | |
|              |  |  ingress)     capture                                          | |
|              |  | payload       Query excerpt: ' OR 1=1-- - matched span not     | |
|              |  |               recorded                                         | |
|              |  | rule - score  waf:sqli (terminal) - numeric score not recorded | |
|              |  | campaign      41 - 3 incidents - nearest: 12:38:51 node 1      | |
|              |  |               (0.12), 11:02:10 node 3 (0.21)                   | |
|              |  | id            node 2 - seq 88,412                              | |
|              |  |                                                                | |
|              |  | REQUEST - RESPONSE                                  UTF-8 v    | |
|              |  | +------------------------------------------------------------+ | |
|              |  | | GET /search?q=%27%20OR%201%3D1-- HTTP/1.1                  | | |
|              |  | | Host: shop.example                                         | | |
|              |  | | User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) ...  | | |
|              |  | | Accept: text/html,application/xhtml+xml,*/*;q=0.8          | | |
|              |  | | Cookie: [redacted]                                         | | |
|              |  | | Response: local denial - no origin response                | | |
|              |  | +------------------------------------------------------------+ | |
|              |  | [Copy as cURL]                                      [Close]    | |
|              |  +--------------------------------------------------------------+ |
|              | ------ | ------------ | -------- | ------ | ----------------- | ---- >|
|              | ------ | ------------ | -------- | ------ | ----------------- | ---- >|
+--------------+-------------------------------------------------------------------+
```

Listing 7 Policy: the ordered rules table and the editor. The tester on the right evaluates a synthetic request against the current policy through the same engine code and names the rule that decided.

```
+-------------------------------------------------------------------------------------+
| SIBUNA                            cluster: edge-eu - 3/3 healthy - admin v - (theme) |
+--------------+----------------------------------------------------------------------+
| Statistics   | POLICY - surface: Shield v - thresholds: 10 / 40 / 5                 |
| Attack events|                                                                      |
| Challenges   | [+ New rule] [Import JSON] [Export]         +------------------------+|
|>Policy       | Rules 12 - file rules 4 (read-only)         | EDIT RULE -            ||
| Nodes        |                                             | protect-checkout       ||
| GeoIP        | = | name   | match     | action | diff | on |                        ||
| Settings     | --+--------+-----------+--------+------+--- | [name               ]  ||
| Audit        | = | ------ | --------- | ------ | ---- | -- | [path pattern       ]  ||
|              | = | ------ | --------- | ------ | ---- | -- | [user agent         ]  ||
|              | = | ------ | --------- | ------ | ---- | -- | [headers (4)        ]  ||
|              | = | ------ | --------- | ------ | ---- | -- | [CIDRs (8)          ]  ||
|              | = | ------ | --------- | ------ | ---- | -- | [action v - weight  ]  ||
|              | = | ------ | --------- | ------ | ---- | -- | [challenge: posw -  ]  ||
|              | = | ------ | --------- | ------ | ---- | -- | [  depth 20         ]  ||
|              | = | ------ | --------- | ------ | ---- | -- |                        ||
|              | = | ------ | --------- | ------ | ---- | -- | [Save] [JSON view]     ||
|              | = | ------ | --------- | ------ | ---- | -- +------------------------+|
|              | = | ------ | --------- | ------ | ---- | -- +------------------------+|
|              | = | ------ | --------- | ------ | ---- | -- | TEST A REQUEST         ||
|              |                                             |                        ||
|              |                                             | [GET /checkout/pay  ]  ||
|              |                                             | [UA: Mozilla/5.0 ...]  ||
|              |                                             | [X-Api-Key: ... -   ]  ||
|              |                                             | [  203.0.113.9      ]  ||
|              |                                             |                        ||
|              |                                             | CHALLENGE - rule       ||
|              |                                             | protect-checkout       ||
|              |                                             | posw depth 20 -        ||
|              |                                             | openings per config    ||
|              |                                             |                        ||
|              |                                             | [Evaluate]             ||
|              |                                             +------------------------+|
+--------------+----------------------------------------------------------------------+
```

Listing 8 Nodes: one card per member with role, health, version, and sparklines, and the two facts an operator must know about cluster semantics.

```
+-------------------------------------------------------------------------------+
| SIBUNA                          cluster: edge-eu - 3/3 healthy - admin v - (theme) |
+-------------+-----------------------------------------------------------------+
| Statistics  | NODES - edge-eu - leader: node 2 - last commit 4,118 - lag 0    |
| Attack events|                                                                |
| Challenges  | +--------------------+  +--------------------+  +--------------------+|
| Policy      | | node 1 - 10.0.0.1  |  | node 2 - 10.0.0.2  |  | node 3 - 10.0.0.3  ||
|>Nodes       | | follower           |  | leader             |  | follower           ||
| GeoIP       | |                    |  |                    |  |                    ||
| Settings    | | healthy - v0.1.0 - |  | healthy - v0.1.0 - |  | storage degraded - ||
| Audit       | | up 3d 4h           |  | up 3d 4h           |  | serving last       ||
|             | |                    |  |                    |  | snapshot           ||
|             | |  _/\_/\__/\_/\     |  |  _/\_/\__/\_/\     |  |                    ||
|             | |                    |  |                    |  |  _/\_/\__/\_/\     ||
|             | | 2,140 req/s -      |  | 2,140 req/s -      |  |                    ||
|             | | 21 MiB - 0.9 core  |  | 21 MiB - 0.9 core  |  | 2,140 req/s -      ||
|             | | bans 312 -         |  | bans 312 -         |  | 21 MiB - 0.9 core  ||
|             | | challenges 64 k -  |  | challenges 64 k -  |  | bans 312 -         ||
|             | | denied 21 k        |  | denied 21 k        |  | challenges 64 k -  ||
|             | |                    |  |                    |  | denied 21 k        ||
|             | | [Drain]            |  | [Drain]            |  |                    ||
|             | | [Clear bans]       |  | [Clear bans]       |  | [Drain]            ||
|             | | [Open console]     |  | [Open console]     |  | [Clear bans]       ||
|             | |   (ext)            |  |   (ext)            |  | [Open console]     ||
|             | +--------------------+  +--------------------+  |   (ext)            ||
|             |                                                 +--------------------+|
|             | +-----------------------------------------------------------------+|
|             | | Challenge verification is issuer-bound: route a solver's fetch and ||
|             | | verify to the same node. Rate limits and spent sets are per node.  ||
|             | +-----------------------------------------------------------------+|
+-------------+-----------------------------------------------------------------+
```

Listing 9 Settings: users with two-factor state, API tokens, page templates, retention, notifications, GeoIP, and about.

```
+-------------------------------------------------------------------------------+
| SIBUNA                          cluster: edge-eu - 3/3 healthy - admin v - (theme) |
+-------------+-----------------------------------------------------------------+
| Statistics  | SETTINGS                                                        |
| Attack events| [USERS - API TOKENS - PAGES - RETENTION - NOTIFICATIONS - GEOIP -     |
| Challenges  |  ABOUT]                                                         |
| Policy      |                                                                 |
| Nodes       | user   | role   | 2FA | last login | state  +------------------------+|
| GeoIP       | -------+--------+-----+------------+------  | ADD USER               ||
|>Settings    | ------ | ------ | --- | ---------- | -----  |                        ||
| Audit       | ------ | ------ | --- | ---------- | -----  | [name              ]   ||
|             | ------ | ------ | --- | ---------- | -----  | [role: viewer v    ]   ||
|             | ------ | ------ | --- | ---------- | -----  | [temporary password]   ||
|             | ------ | ------ | --- | ---------- | -----  | [x] require two-factor ||
|             |                                           +------------------------+|
|             | +--------------------+ +--------------------+ +--------------------+|
|             | | PAGES              | | RETENTION          | | NOTIFICATIONS      ||
|             | | challenge - denied | | minutes 90 d -     | | webhook - syslog -  ||
|             | | - rate limited -   | | incidents 30 d -   | | events: denial     ||
|             | | banned -           | | audit 365 d -      | | spike, ban, node   ||
|             | | overloaded         | | rankings 7 d       | | unhealthy, leader  ||
|             | | edit template -    | +--------------------+ | change             ||
|             | | preview - reset    |                        +--------------------+|
|             | +--------------------+                                          |
|             | +--------------------------------+ +--------------------------------+|
|             | | GEOIP                          | | ABOUT                          ||
|             | | DB-IP Lite - 2026-09 - range   | | v0.1.0 - node 1 - cluster      ||
|             | | count from import - loaded     | | edge-eu - bound 127.0.0.1:9443 ||
|             | | 2026-09-08                     | | behind proxy                   ||
|             | | Update now - attribution shown | | build (example) - storage      ||
|             | | in footer                      | | v0.6.1                         ||
|             | +--------------------------------+ +--------------------------------+|
+-------------+-----------------------------------------------------------------+
```

Listing 10 Challenge dashboard visual layout: independently counted flow stages, accepted solve-time buckets and explicit missing-data coverage. The detailed controls follow.

```
+-------------------------------------------------------------------------------+
| SIBUNA                          cluster: edge-eu - 3/3 healthy - admin v - (theme) |
+-------------+-----------------------------------------------------------------+
| Statistics  | CHALLENGES - all nodes - last hour                              |
| Attack events|                                                                |
|>Challenges  | +-------------------------------+ +-------------------------------+|
| Policy      | | CHALLENGE FLOW - WINDOW TOTALS | | ACCEPTED SOLVE TIME - CLIENT    ||
| Nodes       | |                               | | REPORTED                        ||
| GeoIP       | | +---------------------------+ | | [Hashcash v] -                  ||
| Settings    | | |      Issued - 8,200       | | | [difficulty 16 v]               ||
| Audit       | | +---------------------------+ | |                                 ||
|             | |  +-------------------------+  | |                #                ||
|             | |  |   Submitted - 7,900     |  | |               # #               ||
|             | |  +-------------------------+  | |             # # # #             ||
|             | |   +-----------------------+   | |             # # # #             ||
|             | |   |   Accepted - 7,750    |   | |           # # # # # #           ||
|             | |   +-----------------------+   | |           # # # # # # #         ||
|             | |    +---------------------+    | |       # # # # # # # # # #       ||
|             | |    | Rejected 120 -      |    | | # # # # # # # # # # # # # # # ||
|             | |    | malformed 30        |    | | ------------------------------- ||
|             | |    +---------------------+    | | 0-1 ms - logarithmic powers of  ||
|             | +-------------------------------+ | two - >=16,384 ms               ||
|             |                                   +---------------------------------+|
|             | +-----------------------------------------------------------------+|
|             | | Timing missing 4% - invalid 0.1% - client-reported values are   ||
|             | | untrusted. Issued and submitted can refer to different time-window ||
|             | | cohorts.                                                        ||
|             | +-----------------------------------------------------------------+|
+-------------+-----------------------------------------------------------------+
```

Listing 11 Challenges: flow totals, timing and rejection analysis, with algorithm-aware parameters. Counts are illustrative window totals, not a cohort conversion rate.

```
+-------------------------------------------------------------------------------+
| SIBUNA                          cluster: edge-eu - 3/3 healthy - admin v - (theme) |
+-------------+-----------------------------------------------------------------+
| Statistics  | CHALLENGES - all nodes - last hour - live                       |
| Attack events|                                                                |
|>Challenges  | +-------------------------------+ +-------------------------------+|
| Policy      | | CHALLENGE FLOW                | | INVESTIGATE AND TUNE          ||
| Nodes       | |                               | |                               ||
| GeoIP       | | Issued: 8,200 -> Submitted:   | | REJECTIONS BY CAUSE           ||
| Settings    | | 7,900                         | | Double spend: 52 - Expired: 31 ||
| Audit       | | Accepted: 7,750 - Rejected: 120 | | Fingerprint mismatch: 12 -    ||
|             | | - Malformed: 30               | | Other causes: 25              ||
|             | |                               | | Select a cause -> per-address ||
|             | | ACCEPTED SOLVE TIME (CLIENT   | | records                       ||
|             | | REPORTED)                     | |                               ||
|             | | Algorithm: Hashcash v -       | | Address / node / issued /     ||
|             | | difficulty: 16 v              | | accepted / cause              ||
|             | | Median: 280 ms - p95 bucket:  | | 192.0.2.44 / 2 / 10 / 8 /     ||
|             | | 1,024-2,048 ms                | | expired                       ||
|             | | Timing missing: 4% - invalid: | | Per-address capture missing?  ||
|             | | 0.1%                          | | "Not recorded"                ||
|             | |                               | |                               ||
|             | | Histogram: 16 logarithmic     | | Adaptive difficulty: Show     ||
|             | | buckets                       | | change timeline               ||
|             | | Show bucket counts / Open     | | Solver mode: Wasm / JS        ||
|             | | timing table                  | | fallback / unknown            ||
|             | |                               | |                               ||
|             | | PoSW view uses depth and      | | Edit rule parameters ->       ||
|             | | opening count.                | | preview -> save               ||
|             | | Untrusted device timing; no   | | Runtime limits remain         ||
|             | | security inference.           | | node-local.                   ||
|             | +-------------------------------+ +-------------------------------+|
|             | +-----------------------------------------------------------------+|
|             | | No data: "No challenges in this window". Missing instrumentation: ||
|             | | "Not available". Late submissions may cross windows.            ||
|             | +-----------------------------------------------------------------+|
+-------------+-----------------------------------------------------------------+
```

Listing 12 Attack events grouped by source, including filters, pagination, export and the transition to raw evidence. A paused reader controls when new rows appear.

```
+-------------------------------------------------------------------------------+
| SIBUNA                          cluster: edge-eu - 3/3 healthy - admin v - (theme) |
+--------------+----------------------------------------------------------------+
| Statistics   | ATTACK EVENTS - By source / Raw                                 |
|>Attack events|                                                                 |
| Challenges   | +--------------------------------+ +--------------------------------+|
| Policy       | | SOURCE GROUPS                  | | SOURCE DETAIL                  ||
| Nodes        | |                                | |                                ||
| GeoIP        | | Node: all v - Category: all v  | | 198.51.100.7 - nodes 1, 2      ||
| Settings     | | Address: ________ - Country:   | | 18 recorded incidents - 2      ||
| Audit        | | all v                          | | categories                     ||
|              | | Path: ________ - Period: last  | |                                ||
|              | | 24 h v                         | | Timeline / categories /        ||
|              | |                                | | campaign candidates            ||
|              | | [Show 12 new events] - Live    | | Open raw event -> retained     ||
|              | | paused                         | | evidence                       ||
|              | | Address / incidents / first /  | | Similarity is heuristic, not   ||
|              | | last                           | | attribution.                   ||
|              | | 198.51.100.7 / 18 / 12:00 /    | |                                ||
|              | | 12:41                          | | Ban 24 h / Allow 1 h / Add to  ||
|              | | 192.0.2.44 / 9 / 11:30 / 12:39 | | group                          ||
|              | |                                | | Preview overlap and effective  ||
|              | | Select source -> filtered raw  | | precedence                     ||
|              | | events                         | | Confirm -> applied per-node    ||
|              | | Country: Unknown for these     | | revision                       ||
|              | | example IPs                    | |                                ||
|              | |                                | | Undo 30 s -> new audited       ||
|              | | Previous / Page 1 / Next -     | | mutation                       ||
|              | | Export CSV                     | | Export omits credentials and   ||
|              | | Export respects filters and    | | redacted data.                 ||
|              | | size limits.                   | +--------------------------------+|
|              | +--------------------------------+                                 |
|              | +-----------------------------------------------------------------+|
|              | | Empty: adjust filters. Retention gap, dropped incidents and stale  ||
|              | | replica state are shown above the list.                        ||
|              | +-----------------------------------------------------------------+|
+--------------+----------------------------------------------------------------+
```

Listing 13 Policy modes, limits and IP groups complement the rule editor. Audit mode continues evaluation; country operations are capacity-checked before commit.

```
+-------------------------------------------------------------------------------+
| SIBUNA                          cluster: edge-eu - 3/3 healthy - admin v - (theme) |
+--------------+----------------------------------------------------------------+
| Statistics   | POLICY - Rules / Inspection / Limits / IP groups                |
| Attack events|                                                                 |
| Challenges   | +--------------------------------+ +--------------------------------+|
|>Policy       | | INSPECTION AND LIMITS          | | IP GROUPS AND COUNTRY ACTION   ||
| Nodes        | |                                | |                                ||
| GeoIP        | | Category / mode                | | Prefix / action / expiry /     ||
| Settings     | | SQL injection / Enforce v      | | provenance                     ||
| Audit        | | XSS / Audit v                  | | 192.0.2.0/24 / deny / 1 h /    ||
|              | | Path traversal / Enforce v     | | operator                       ||
|              | | RCE / Disabled v               | | Add prefix / edit / remove     ||
|              | |                                | |                                ||
|              | | Audit logs a finding then      | | COUNTRY BUILDER                ||
|              | | continues evaluation.          | | Country: select v - GeoIP      ||
|              | | Another enforcing rule can     | | generation: current            ||
|              | | still deny.                    | | Action: Deny v - Duration: 24  ||
|              | |                                | | h v                            ||
|              | | LIMITS - target node: node 2 v | | Preview CIDRs / overlaps /     ||
|              | | Current GCRA: rate / window /  | | trie-node usage                ||
|              | | ban duration                   | |                                ||
|              | | Terminal rules own additional  | | Reject if full; never silently ||
|              | | node-local quotas.             | | truncate.                      ||
|              | |                                | | Challenge needs explicit       ||
|              | | Review changes -> Save expected| | supported rules.               ||
|              | | revision 17                    | |                                ||
|              | +--------------------------------+ | Confirm / Cancel - Conflict?   ||
|              |                                    |                                ||
```

```
|              |                                  | reload and diff                |
|              |                                  | Committed revision != applied  |
|              |                                  | on every node.                 |
|              |                                  +--------------------------------+|
|              | +-------------------------------------------------------------------+|
|              | | Viewer: edits disabled. Invalid input: inline error. Full engine:  |
|              | | reject. Concurrent edit: show conflict before retry.               |
|              | +-------------------------------------------------------------------+|
+--------------+-----------------------------------------------------------------------+
```

Listing 14 GeoIP is a complete source/import workflow, with validation, attribution, progress, failure recovery and policy-generation pinning.

```
+-------------------------------------------------------------------------------------+
| SIBUNA                           cluster: edge-eu - 3/3 healthy - admin v - (theme) |
+--------------+----------------------------------------------------------------------+
| Statistics   | GEOIP - country enrichment                                           |
| Attack events|                                                                      |
| Challenges   | +--------------------------------+ +--------------------------------+|
| Policy       | | CURRENT DATABASE               | | UPDATE DATABASE                ||
| Nodes        | |                                | |                                ||
|>GeoIP        | | Provider: ip-location-db       | | Download -> validate -> stage  ||
| Settings     | | user-country v                 | | -> activate                    ||
| Audit        | | Source version: 2026-09-09     | | Progress: 2 of 4 stages -      ||
|              | | (example, daily)               | | Cancel                         ||
|              | | Active generation: 7 - Loaded: | | Bounded bytes and rows; one    ||
|              | | 12:00 UTC                      | | import at a time               ||
|              | | IPv4 / IPv6 ranges: counts from | |                                ||
|              | | loader                         | | Preview source, licence,       ||
|              | | SHA-256: copy digest           | | checksum, range count          ||
|              | | Licence: PDDL 1.0 -            | | Errors keep the prior          ||
|              | | Attribution: none (DB-IP: CC BY | | generation active.            ||
|              | | 4.0)                           | | Retry / View diagnostic        ||
|              | |                                | |                                ||
|              | | Country only; no individual    | | Publisher SHA-256 files        ||
|              | | coordinates.                   | | verified per source file       ||
|              | | Private/reserved/unmapped      | | One HTTPS redirect hop to the  ||
|              | | addresses: Unknown             | | fixed asset host               ||
|              | |                                | |                                ||
|              | | Lookup address: ________ [Look | | Update data / Review affected  ||
|              | | up]                            | | country policies               ||
|              | | Result: country / unknown /    | | Policy prefixes stay pinned    ||
|              | | generation                     | | until approved.                ||
|              | +--------------------------------+ +--------------------------------+|
|              | +-------------------------------------------------------------------+|
|              | | No database: "GeoIP unavailable"; dashboard globe shows only       |
|              | | outline and Unknown totals. No invented locations.                 |
|              | +-------------------------------------------------------------------+|
+--------------+-----------------------------------------------------------------------+
```

Listing 15 Audit with before/after evidence, safe exports and conflict-checked rule revert. Local commands show intent and completion separately.

```
+-------------------------------------------------------------------------------------+
| SIBUNA                           cluster: edge-eu - 3/3 healthy - admin v - (theme) |
+--------------+----------------------------------------------------------------------+
| Statistics   | AUDIT - activity and policy history                                  |
| Attack events|                                                                      |
| Challenges   | +--------------------------------+ +--------------------------------+|
| Policy       | | ACTIVITY                       | | SELECTED CHANGE                ||
| Nodes        | |                                | |                                ||
| GeoIP        | | Actor: all v - Action: all v - | | Actor: alice - operator -      ||
| Settings     | | Period: 24 h v                 | | address recorded               ||
|>Audit        | | Subject: ________ - Node: all v | | Policy p1 - revision 17 -> 18 ||
|              | |                                | |                                ||
|              | | Time / actor / action / subject | | Before: action challenge;      ||
|              | | / result                       | | difficulty 16                  ||
|              | | 12:41 / alice / policy edit /  | | After: action deny             ||
|              | | p1 / committed                 | | Reason: operator description   ||
|              | | 12:40 / admin / drain / node 2 | |                                ||
|              | | / completed                    | | Applied: node 1 ok - node 2 ok ||
```

```
|              | | 12:38 / ci / export / events /  | | - node 3 pending               ||
|              | | completed                       | | Review policy revision /       ||
|              | |                                 | | Revert this change             ||
|              | | Previous / Page 1 / Next -      | |                                ||
|              | | Export                          | | Revert restores the document   ||
|              | | Retention: 365 days - old       | | recorded before revision 18 as ||
|              | | records expire                  | | revision 19 with a fresh       ||
|              | | Append-only for users, not      | | audit.                         ||
|              | | tamper-proof.                   | | Rejected if revision 18 is no  ||
|              | +---------------------------------+ | longer current; Policy history ||
|              |                                     | offers compare and rebase.     ||
|              |                                     | Secrets and full token values  ||
|              |                                     | never displayed.               ||
|              |                                     +--------------------------------+|
|              | +-----------------------------------------------------------------------+|
|              | | Local action detail: request id, intent, target acknowledgment and ||
|              | | failure reason; no false atomicity claim.                           ||
|              | +-----------------------------------------------------------------------+|
+--------------+-------------------------------------------------------------------------+
```

Listing 16 Settings forms cover credentials, templates, retention and notifications, with separate read-only About information and safe previews.

```
+-------------------------------------------------------------------------------------+
| SIBUNA                          cluster: edge-eu - 3/3 healthy - admin v - (theme) |
+--------------+----------------------------------------------------------------------+
| Statistics   | SETTINGS - Users / Tokens / Pages / Retention / Notifications / About |
| Attack events|                                                                      |
| Challenges   | +--------------------------------+ +--------------------------------+|
| Policy       | | USERS AND API TOKENS           | | OPERATIONAL SETTINGS           ||
| Nodes        | |                                | |                                ||
| GeoIP        | | User: alice - role: operator v | | TEMPLATES - denied v - bounded ||
|>Settings     | | TOTP: enrolled - last login:   | | placeholders                   ||
| Audit        | | 12:00 UTC                      | | Edit / sandboxed preview /     ||
|              | | Disable user / reset password / | | reset / save                   ||
|              | | revoke sessions                | | No executable scripts or       ||
|              | |                                | | arbitrary imports              ||
|              | | Token label: deploy-ci - role: | |                                ||
|              | | operator v                     | | RETENTION - traffic 90 d -     ||
|              | | Expiry: date/time - scope:     | | incidents 30 d                 ||
|              | | policy only                    | | Rankings 7 d / 512 MiB - audit ||
|              | | Create -> show secret once ->  | | 365 d                          ||
|              | | copy -> close                  | | Estimate footprint -> review   ||
|              | | Existing tokens: id / scope /  | | -> save                        ||
|              | | expiry / revoke                | |                                ||
|              | |                                | | NOTIFICATIONS - destination    ||
|              | | Viewer role: inspect, cannot   | | type: webhook v                ||
|              | | change settings.               | | URL / masked secret / events / ||
|              | | Administrator changes require  | | cooldown                       ||
|              | | recent auth.                   | | Test destination -> show       ||
|              | |                                | | result -> save                 ||
|              | | About: node/version/build/liste | | Node unhealthy / leader change ||
|              | | ner/storage                    | | / denial spike                 ||
|              | | Never expose secrets or        | | Bounded retries; one cluster   ||
|              | | arbitrary environment.         | | notifier lease                 ||
|              | +--------------------------------+ +--------------------------------+|
|              | +-----------------------------------------------------------------------+|
|              | | Validation is inline; save has pending/success/error states. Slow  ||
|              | | notifications never run in data-plane threads.                      ||
|              | +-----------------------------------------------------------------------+|
+--------------+-------------------------------------------------------------------------+
```

Listing 17 Authentication states. The public sign-in surface loads no globe, GeoIP or telemetry; the dashboard starts only after all required authentication steps succeed.

```
                                SIBUNA - Sign in

+-------------------------+ +-------------------------+ +-------------------------+
| 1 - CREDENTIALS         | | 2 - REQUIRED            | | 3 - SUCCESS / EXPIRY    |
|                         | | VERIFICATION            | |                         |
| Username                | |                         | | Success -> Traffic      |
```

```
| [____________]           | | Authenticator code       | | overview                 |
| Password                 | | [____________]           | | Load globe + open        |
| [************]           | | [Verify]                 | | streams                  |
|                          | |                          | |                          |
| [Sign in]                | | Use recovery code        | | Expired -> Sign in again |
|                          | |                          | | Preserve safe return     |
| Invalid credentials:     | | First login: change      | | route                    |
| retry                    | | temporary password;      | |                          |
| Rate limited: retry      | | enroll TOTP when         | | No users? Run init-admin |
| after Ns                 | | required.                | | locally; no public       |
+--------------------------+ +--------------------------+ | account creation.        |
                                                          +--------------------------+
+-------------------------------------------------------------------------------------+
| Authentication only: no globe assets, telemetry connection, country data, cluster  |
| health or traffic on the sign-in page.                                              |
+-------------------------------------------------------------------------------------+
```

Listing 18 Kiosk after a one-time code is entered in the sign-in form: full-screen live globe, coverage and traffic/attack summaries. Expired access returns to sign-in; no mutation controls are present.

```
+-------------------------------------------------------------------------------------+
| SIBUNA - edge-eu - Traffic / Attacks - 3/3 reporting - live - last update 1 s       |
+-------------------------------------------------------------------------------------+
+-----------------------------------------------+ +---------------------------------+
| LIVE EARTH GLOBE - TRAFFIC / ATTACKS          | | LAST 60 SECONDS                 |
|                                               | | Requests: 128 k (example)       |
|                    +----------------------+   | | Recorded incidents: 128         |
|     .-~~~~~-.      | COUNTRIES            |   | | Unknown country: 4%             |
|   .' o ox    '.    | Germany - 2,560      |   | +---------------------------------+
|  /    .      x \   | India - 1,920        |   | +---------------------------------+
| |   .  o        |  | Brazil - 1,280       |   | | MODULE TRENDS                   |
| | o      .      |  | Unknown - 4%         |   | | Inspection / reputation /       |
|  \      o      /   |                      |   | | limits                          |
|   '.         .'    | Samples - p=1/64     |   | | Challenges / bans / honeypot    |
|     '-~~~~~-'      | Loss: 0 (example)    |   | | Read-only - no payload detail   |
|                    +----------------------+   | +---------------------------------+
|                    +----------------------+   |
|                    | Rotate / Pause /     |   |
|                    | Reset                |   |
|                    +----------------------+   |
+-----------------------------------------------+
+-------------------------------------------------------------------------------------+
| Exit kiosk - session expiry visible - no URL bearer token - stale stream freezes    |
| with age; GeoIP unavailable shows outline only                                      |
+-------------------------------------------------------------------------------------+
```

Listing 19 Responsive and data-state variants. Navigation remains labelled; the mobile landing page places the globe and country table in a vertical flow.

```
+--------------------------------+ +-----------------------------------------------+
| +----------------------------+ | | LOADING / EMPTY                               |
| | Menu - SIBUNA - admin v    | | | Fixed-size skeleton; no fabricated zeros. Once |
| +----------------------------+ | | loaded: "No traffic in this window". First use |
| +----------------------------+ | | preserves navigation and setup links.         |
| | Traffic - all nodes        | | +-----------------------------------------------+
| | 24 h - Live / Pause        | | +-----------------------------------------------+
| +----------------------------+ | | GEOIP UNAVAILABLE                             |
| +-------------+ +------------+ | | Earth outline only; Unknown totals, provider  |
| | 128 k       | | 128        | | | state and admin setup link. Country controls  |
| | Requests    | | Incidents  | | | disabled with explanation.                    |
| +-------------+ +------------+ | +-----------------------------------------------+
| +----------------------------+ | +-----------------------------------------------+
| | Globe - Traffic / Attacks  | | | DISCONNECTED / PARTIAL CLUSTER                |
| |                            | | | Freeze last values; display age and 2/3       |
| |   .-~~-.    Rotate         | | | reporting. Retry with backoff. Resnapshot     |
| |  / o x  \   Flat map       | | | before clearing stale state.                  |
| | |  o .   |                 | | +-----------------------------------------------+
| |  \  o   /                  | | +-----------------------------------------------+
| |   '-~~-'                   | | | ERROR / PERMISSION / OVERFLOW                 |
| +----------------------------+ | | Inline diagnosis and retry; viewer actions    |
| +----------------------------+ | | disabled; truncated history marked. Keyboard  |
```

```
| | Countries (down)           | | | focus persists across live patches.             |
| | Timeline (down)            | | +-------------------------------------------------+
| | Full labels in menu        | |
| +----------------------------+ |
+--------------------------------+
```

Coverage	Required variants and navigation
Statistics	Signed-in globe/timeline, Traffic and Security tabs, sampled/incident modes, country drill-down, kiosk, mobile, GeoIP missing and stale/partial cluster.
Events and Challenges	Grouped and raw events, evidence detail, source actions, export/pagination, challenge flow/timing/cause, missing instrumentation and retained-history gaps.
Policy and Nodes	Rule editor/tester, inspection/limits/groups/country builder, revision conflict; node drill-down, drain preview/confirm/result and clear-local-bans result.
Settings and Audit	Users, tokens, TOTP/recovery, templates, retention, notifications and About; audit diff/revert and local-command intent/completion.
Authentication and shared states	Credentials, setup, forced password change, TOTP, recovery, expiry; loading/empty/error/forbidden; labelled responsive navigation, focus and reduced motion.

18. The Build Pipeline

`build.zig` gains a `console` concern (`build/console.zig`, following zenfmt's one-file-per-concern layout), wired by the existing `AppModules` helper.

Step	What it does
`-Dconsole` (defaults to storage enabled)	Compiles `libs/serve`, `libs/console`, and the interface module into the daemon; `-Dconsole=false` removes every console symbol and the `--console` flags.
`console-ui` (implicit)	Compiles `apps/console-ui/src/main.zig` for `wasm32-freestanding` at `ReleaseSmall`, warns above 448 KiB, enforces the 512 KiB artifact ceiling, and embeds the bytes.
`zig build console-assets`	Runs `npm ci` and `npm run build` in `apps/console-ui/web/` through `b.addSystemCommand`, producing `assets/console.css` from `tailwind.css` with Tailwind 4 and the daisyUI 5 plugin, using explicit Tailwind source paths for Zig render files and HTML snippets, with complete class names in those sources; daisyUI components are restricted with its `include` configuration. The step then writes `assets/MANIFEST.md` with the SHA-256 of every asset.
Digest gate (in `zig build test`)	`tools/console_assets.py check` hashes both build inputs (render sources, HTML snippets, the snippet renderer, CSS configuration, package lock and scripts) and outputs against `MANIFEST.md`; output digests alone cannot detect stale CSS. A plain `zig build` therefore needs no npm; only `console-assets` does, and CI runs it and checks the tree is clean.
`zig build console-test`	Golden tests of the interface module compiled natively (rendered HTML per page and per event), protocol round-trip tests, and the kernel's HTTP and WebSocket tests with an in-process client.
`zig build console-e2e`	Boots a daemon with `--console` on loopback, runs setup, login, a WebSocket subscription, a policy edit, and asserts the engine rebuild and the audit row; part of `zig build test` when console support is enabled.
`zig build console-impact`	The isolation gate in "Process model and the isolation contract" through `benchmarks/console_impact.py`: builds a console-free and a console binary, runs one compiled-out, disabled, idle or eight-dashboard configuration at a time, interleaves wrk rounds in rotating order over admitted, challenged, denied and policy-reload workloads, and reports pass, fail or inconclusive

Step	What it does
	with a bootstrap interval; `-- --quick` for a smoke run, `-- --cluster` for the three-node case.

`package.json` pins exact compatible versions of `tailwindcss` 4, `@tailwindcss/cli` 4 and `daisyui` 5; `package-lock.json` is committed. npm runs only inside `console-assets`, never in the default graph, so a contributor without Node can build, test, and run the daemon and the console with the committed stylesheet.

19. Security Considerations

- The console is an administrative surface and is bound to loopback by default; off-loopback exposure requires an explicit address and `--console-behind-proxy` with TLS at the ingress. The data plane's own listener never serves console routes (I1), so a console vulnerability cannot be reached through the protected site.
- All state-changing routes require a session or token with an adequate role (cookie-authenticated requests also require the CSRF header), and are rate limited; all are audited. Password hashing concurrency, memory and request rates have independent bounds; session digests mean a database read exposure does not yield usable sessions.
- The interface module renders through an escaping writer; the content security policy forbids inline script and remote resources; the WebSocket accepts only same-origin upgrades; the shell sets `X-Frame-Options: DENY`.
- The policy tester evaluates through the real engine code but on the console thread against a private engine instance built from the same configuration, file fallback and current tables, never against the live slot.
- GeoIP enrichment is country-only; incident rows still contain client addresses and bounded request data. The loader verifies HTTPS and a publisher/operator digest when supplied, and the loaded set replaces the previous one atomically.
- Drain and clear-local-bans follow the audited control-command protocol. Rich incident capture redacts sensitive headers and query/body fields before persistence; previews and "copy as cURL" use escaped, redacted data and mark incomplete requests. Operator templates are constrained placeholders, not executable script, and preview inside a sandboxed frame. Webhook destinations and node probes use allowlisted schemes/hosts/ports with redirect and DNS-rebinding checks; credentials never appear in audit payloads.

20. Performance Budget

These are proposed targets to validate, not measured properties or hard real-time guarantees. Latency includes scheduling, contention and replication; expose age and backlog when targets are missed. The default idle budget excludes active hashing/import work but includes the configured slots, queues and optional GeoIP dataset. Record active peak RSS separately.

Quantity	Bound	Mechanism
Console resident memory, idle	Target to size and measure	Six topic rings and one browser-statistics trigger ring reserve 14 MiB of payload plus metadata and cached views; add connection queues, the owned dashboard frame, snapshot buffers, traffic queue, service stacks, SQL results, GeoIP generations, and the 19 MiB Argon2 workspace
Console CPU, idle	$\leq$ 2 % of one core	4 Hz sampler, 1 Hz coalescing, 5 s probes
Data-plane throughput with 8 live dashboards	within 1 % of no console	I1, I2, I5; measured by `console-impact`
Data-plane p99 with 8 live dashboards	within 10 %	Same
Statistics delta latency	$\leq$ 1.25 s	Sampler period plus 1 Hz broadcast

Quantity	Bound	Mechanism
Incident to dashboard	Target $\leq$ 2.25 s + commit delay without backlog	"The incident tap"; slow storage and replication can exceed this
Policy edit to rebuilt engine on every node	Target: commit/apply + next successful tick	SID 0005 path
Interface module size	Warn above 640 KiB; $\leq$ 768 KiB	`ReleaseSmall`, uncompressed artifact guardrail; review with browser timings
Browser experience	LCP $\leq$ 2.5 s; INP $\leq$ 200 ms; CLS $\leq$ 0.1	Published user-experience targets at the 75th percentile, separately for mobile and desktop; recorded lab checks do not establish field acceptance
Page render (statistics, 3,600-point timeline)	$\leq$ 5 ms in the module	Bounded writer, per-panel versions
WebSocket subscribers per console	64	Slot table; `503` beyond

21. Delivery Plan

The phases define dependency order, not a progress ledger. Implementation history belongs in git. SID 0001 defines completion through implementation, verification and benchmark gates. The dated launch scope below records the explicit exception for this launch; the remaining performance condition still governs enabling the console in production.

Phase 1: Kernel, authentication, statistics (planned)

`libs/serve` with HTTP, assets, and WebSocket; `libs/console` with auth, sessions, audit, the sampler, `traffic_minutes`, and the `stats` topic; the interface module with the shell, setup, login, and the statistics page; `console-assets` and the digest gate; the e2e test; the impact gate with the stated throughput/p99 thresholds. A single node exposes currently available counters; unavailable panels say so. Include TOTP before permitting off-loopback access and keyboard/focus/accessibility support from this phase.

Phase 2: Events, policy, challenges, GeoIP (planned)

The incident tap and `events` topic with the detail drawer and actions; the policy editor, tester, import and export, and IP groups over `policies` and `ip_reputation`; the challenge funnel with the solve-time histogram; the traffic sample ring, Space-Saving rankings and the sampled panels; per-category inspection modes; the GeoIP loader, lookup, map, and country actions; retention.

Phase 3: Cluster (planned)

The `nodes` table and page, health probes, node-to-node live buckets, leader awareness, drain, per-node views on every page, and the cluster case of the impact gate through `benchmarks/console_impact.py --cluster`.

Phase 4: Operations (planned)

API tokens, notification webhooks and syslog, exports, editable page templates, the kiosk view, the audit page, dark theme polish, keyboard navigation and screen-reader labels, and the operator guide in the book (a new chapter in Part IX with the wireframes replaced by screenshots of the built console).

22. Verification

- **Unit.** Router matching, JSON writer bounds, Argon2id and token digests, CSRF, WebSocket framing and fragmentation against RFC 6455 vectors (standard-library helper tests alone are insufficient), ring and cursor semantics, sampler deltas across counter wrap, minute folding, GeoIP range parsing and lookup, retention windows.
- **Golden.** Every page and every event-driven patch of the interface module compiled natively, compared byte-for-byte with committed HTML; a change to markup is a reviewed diff.
- **End-to-end.** The `console-e2e` scenario above, plus: session expiry, role refusal, rate limit on login, a slow subscriber receiving `dropped`, a stateless policy tester result agreeing with a live request's `X-Sibuna-Rule` under controlled identical inputs and configuration, a country block appearing in the trie, and a cluster run in which a rule saved on node 1's console changes node 3's decision (`tools/console_cluster_test.py`, run by `console-e2e` under `-Dcluster=true`: membership, probes, leader loss, lost quorum answering `CONSOLEQUORUM`, rejoin, cross-node revocation and local-command isolation).
- **Impact.** The `console-impact` gate on every change to `libs/serve` or `libs/console`.
- **Principles.** The golden tests assert the mechanical rules: every page passes the trunk test (product, cluster and node, page, section, way back present in the rendered shell, R2); decision colours appear only through the four semantic classes (R8); tiles carry a deviation marker and a sparkline (R9, R11); numbers render with tabular figures and separators (R12); no verdict element renders without its reason element (R14); every destructive action renders with a duration or a confirmation (R18). The judgement rules are evaluated with human operators using two scripted tasks (browser automation checks mechanics, not human comprehension): a five-second look at Statistics must let a reader name the anomalous module, and "find why request X was denied" must complete in three clicks from the shell.
- **Telemetry correctness.** Inject counter resets, issuer-order inversions, duplicate peer buckets, partial minutes, sample loss, and cross-window challenge solutions. Check sketch estimates against exact sample counts and merge error bounds; exercise the Unknown bucket.
- **Globe and authentication.** Assert zero globe/GeoIP/telemetry loads before successful login, including failed login, TOTP and forced-change states. Test Traffic/Attacks switching, missing GeoIP, country coverage, back hemisphere clipping, poles, antimeridian crossings, keyboard centering, pause, stale/reconnect and sign-out stream teardown. Record geometry vertex, linear-memory and render-time budgets on desktop and a low-end device.
- **Abuse and failure.** Test bounded distributed login load, revoked sessions on followers, fragmented/invalid WebSockets, unsolicited delivery while the reader blocks, 64 subscribers with HTTP slots remaining, SQL deadline/backpressure, GeoIP failed activation, trie-full country rejection, revision conflicts and unauthenticated probe/webhook destinations.
- **Document.** Compile this source to PDF and to page PNGs with Typst; inspect every wireframe for clipping, overlap, navigation completeness and the separate authentication shell.
- **Browser.** A minimal Chromium script (the harness family of the benchmarks) loads the console, logs in, and checks that tiles update, kept outside `zig build test` because it needs a browser.

Document review is reproducible without building the daemon:

```
mkdir -p docs/build/review-0007
typst compile --root docs docs/sid/records/0007-console-management-interface.typ docs/build/review-0007/
console.pdf
typst compile --root docs docs/sid/records/0007-console-management-interface.typ 'docs/build/review-0007/
page-{0p}.png' --ppi 120
typst compile --root docs docs/sid/figures/0007-console-landing-preview.typ docs/build/review-0007/
landing.png --ppi 160
```

23. Resolved Design Decisions

The former open questions are resolved as follows; implementation must verify the stated bounds rather than reopen the architecture implicitly.

1. **Live cluster transport:** direct authenticated TLS management streams. Membership, applied revisions and probe health use replicated rows and explicit probes; ephemeral node statistics use direct authenticated management WebSockets on a separate `/console/peer` route and bounded peer quota.

Authenticate node identity against configured membership, using the domain-separated HMAC transcript over certificate-validated TLS. The consensus PSK is not a browser bearer token. Never use a server-only masked-frame reader as the outbound client: peer clients must mask writes and accept unmasked server frames. Keep ephemeral statistics out of consensus and require fresh epoch/sequence metadata; disconnected peers become stale, never healthy zeros.

2. **Solve timing:** add optional telemetry to the existing verification POST as specified in "The challenge funnel". No separate public endpoint on the privileged console listener, no second browser request, and no trust in client timing for security decisions. Missing telemetry is counted.
3. **Retention:** default traffic/challenge/country minutes to 90 days, ranking sketches to 7 days, incidents to 30 days and audit to 365 days. Three continuously running nodes yield 388,800 node-minute rows per 90-day table before boot/bin multiplicity. Ranking sketches can dominate storage (up to 256 keys × kinds × node-minutes); enforce explicit byte/row quotas, batch deletion and storage backpressure. Default to a 512 MiB ranking-store quota; on exhaustion shorten retained ranking history with a visible coverage boundary. Coalesce minute writes, prefer incident/control work over telemetry, and measure replicated disk, journal and compaction costs. Never assume a SQLite row count establishes capacity.
4. **Stylesheet:** ship only the pinned, curated sheet and its input/output manifest. The explicit `console-assets` step regenerates it reproducibly; ordinary builds use committed assets. Themes are reviewed source changes through the same build, not an unbounded full-CSS option.
5. **Globe:** implement the bounded orthographic SVG view in "Live earth globe on the landing page" with country-only traffic/attack views after successful login, 1 Hz updates, accessible ranked table, manual rotation and honest unavailable/stale states. Its geometry, attribution, seam clipping and render budget are release checks.
6. **Storage ownership and local commands:** retain a single Zaxonlite owner and add bounded mailboxes, preflight validation and revision acknowledgments. SQL query cancellation or separately owned read snapshots is an implementation prerequisite for heavy forensics. This design cannot promise panic isolation inside the single daemon process.

Remaining work consists of implementation and acceptance measurements: storage adapter concurrency/cancellation validation, memory sizing, provider import tests, browser protocol conformance, globe projection tests, operator usability sessions and the impact matrix. No unmeasured target in this record is a release claim.

24. Operational Contracts and Trade-offs

24.1. Retained observations

Primary Traffic tiles default to the selected nodes' last 24 hours of closed-minute history. One-hour, seven-day, ninety-day and live-boot views make the observation period explicit. A completed scan stays visible with its age while the next scan runs, one minute after completion. The globe, request timeline and sparklines retain their independent live 60-second window. Missing node history is never silently omitted from coverage.

The compact minute-summary API returns at most 96 records plus one lookahead per indexed storage query, below the existing 100-row and 64 KiB bounds. Shared native/Wasm arithmetic preserves exact counters, cursor ordering, partial intervals and overlaps across node boots. The comparison workflow freezes two UTC windows and permits sixteen pages per side per explicit batch. Longer scans require continuation. Percentages need complete, non-overlapping, equal-duration coverage on both sides and use rates normalized by observed milliseconds. The minute format does not retain proxy mode, so historical origin-response comparisons remain unavailable. Decimal strings preserve counters beyond JavaScript's exact integer range.

Complete path-frequency sketches are retained as versioned SBR1 archives, split into bounded chunks and published only after checksum and semantic validation. The 512 MiB charged quota bounds reservations rather than physical database size; journal and cache costs remain separate. Cross-window rankings must merge every retained counter, never just display winners. The merge follows Algorithms 3 and 4 of Cafaro, Pulimeno and Tempesta, A Parallel Space Saving Algorithm for Frequent Items. Common keys add estimates and errors; absent keys add the other sketch's minimum (zero unless full), then the largest

256 estimates survive. Inputs must represent disjoint sample populations. Exact-population tests establish the implementation's error and inclusion bounds through repeated merges; archive identity and cursor ordering supply deduplication separately. Repeated cumulative queue-loss observations cannot be summed into an exact interval loss. Missing archives, restart overlaps and quota-shortened history remain visible.
Retained ranking reads return one full archive plus a descending minute/digest cursor. An indexed two-row lookahead and at most two ten-row chunk queries fit the storage facade's row and byte limits. The mailbox owns each bounded archive payload until transfer or release; read authorization and retention are checked before and after materialization. Native and Wasm consumers share the codec and merge arithmetic. Explicit comparison actions read at most sixteen archives total, with one outstanding request. Continuation keeps both windows frozen; invalid archives never partially update a displayed population. Node 0 includes retired nodes. Display rows show lower-upper sample bounds and cannot imply exact counts or complete coverage. The browser event buffer is derived from the maximum hex archive plus metadata and envelope headroom. Complete decoding and merge candidates live in caller-owned event scratch, not the Wasm call stack; native consumers may use the same codec and arithmetic with stack workspaces. The four-MiB browser memory ceiling is independent of the artifact-size review threshold.

24.2. Rule observations

A rule hit is a successful declarative matcher evaluation. WEIGH matches count alongside the first terminal match; inspection or reputation decisions that prevent rule evaluation produce no declarative hits. Private policy tests do not increment these counters. Match indices belong to a pinned immutable engine generation, so publication cannot relabel an in-flight request. The request path records bounded bits and increments generation-owned counters only.
The storage owner samples counters once per second and seals ending-minute observations, using the same interval convention as Traffic history. It copies rule identities and pending counts before an old engine arena can be reused. Four owned pending frames and eight rows per storage step bound backlog and work; exhausted capacity remains visible as unconfirmed history and must not delay policy publication. Immutable node/boot/sequence/rule identities make retries idempotent. Observations and their hour/day summaries commit together; arithmetic overflow makes a summary unavailable rather than wrapping or rounding an exact counter.
Rule history uses the minute-retention setting. Indexed reads return at most 48 observations plus lookahead per page, and comparisons retain their rule, node, policy-revision and UTC boundaries across continuation. The smaller read bound leaves room for the replicated transport's typed cell envelopes. Current-day summaries exclude open or future interval cohorts; older rollups without an exact ending minute use the bucket's end conservatively. Startup, cutover, clock changes and missing writes prevent a complete-coverage claim. Hits-today values and sparklines describe recorded intervals; comparing before and after an edit does not establish that the edit caused a change in traffic.

24.3. Management consistency

The Persistent storage owner executes typed, owned mailbox operations. Handlers receive no raw database connection. Execution-time authorization and revision checks fence queued work; cancellation transfers or releases ownership rather than leaving borrowed caller memory. A deadline ends the caller's wait, not an executing database query. Storage uses the supported Zaxonlite prepared-query and replicated protocol facilities with explicit row and byte bounds.
Policy edits, ordering, imports, reputation changes and country replacements validate a full private candidate including file fallbacks. Database changes and redacted audit records commit together. Applied revisions are node acknowledgments; failed materialization preserves the previous engine. Local drain and ban-clearing commands record intent and completion separately. Database commit and runtime effects are not a single atomic action.
Country replacement pins the reviewed GeoIP generation and policy revision, enumerates added, retained and removed prefixes, and refuses independent ownership conflicts or capacity overflow. An import never silently changes country rules. Notifications and maintenance use fenced leases, bounded destinations, retry queues and explicit completion; secrets are sealed and omitted from audit records. A kiosk code is exchanged through a form for an expiring scoped cookie, never placed in a URL or browser storage.

24.4. Browser and peer state

The authenticated browser uses six bounded topics over one WebSocket. Snapshot watermarks, subscription epochs, sequence gaps and atomic reassembly prevent mixing old and new scopes. Live patches preserve unsent form values and focus. Fragment history contains page names only; authentication and authorization precede route restoration. Theme and density preferences may persist, but credentials and private drafts do not enter local storage.

Direct management WebSockets use certificate-validated TLS and a separate, domain-separated peer key. A peer sends only its own observations. Configured node, boot, sequence and interval identity fence duplicates and stale data. Retained seconds and current-minute path queries select one issuer; missing peers stay unavailable and a restart invalidates their cursors. Aggregate-only kiosk Security queries cannot request source addresses, paths or payloads.

25. Acceptance and Open Questions

SID 0001 normally requires implementation on main and satisfied verification and benchmark gates before Committed status. The launch-scope exception below does not establish a full performance pass; the observability requirements it deferred were completed afterwards (see “Post-launch completion”). Test entry points are `zig build test`, `console-test`, `console-ui-e2e`, `console-e2e` with clustering enabled, and `console-impact`. Formatting and the SID, book and HTML builds verify structural and documentation contracts. Exact test history belongs in git; measured records under `benchmarks/results/` carry source identity, conditions and uncertainty.

Retained ranking and per-rule comparisons follow the bounded archive and observation contracts above. R16 requires frozen periods, revision-aware rule identity, visible missing coverage and private-tester exclusion; storage and live-daemon tests exercise these properties. Conditional panels without captured fields must remain unavailable. Browser review must cover all defined workflows and failure states, accessibility, representative device conditions and the two operator-comprehension tasks; an automated mechanical check cannot prove comprehension.

The impact workload requires eight authenticated clients receiving live frames and recently completed daily scans. Single-issuer views also query rankings and retained seconds. Cluster measurements require all configured peer directions, stable boots, advancing watermarks and loaded geography. Throughput degradation must be at most 1%, with p99 increase at most 10%, under the defined workload matrix. Missing delivery, unstable baselines or inconclusive confidence intervals do not pass. Primitive baselines and smoke runs cannot substitute for this gate. These criteria remain the definition of a full pass; the launch scope below records the project owner’s decision of 2026-09-11 and the conditions attached to it.

25.1. Query and authentication observation bounds

Security aggregates use an operator-selected local statement allowance through `--console-query-steps` (100,000 to 50,000,000 steps, default four million). Point reads retain their smaller budget. Cluster reads use the supported Zaxonlite RPC facade and its fixed ten-million-step server limit; the local option cannot override it. VM steps bound work, not wall-clock time, and exhaustion produces an unavailable result with a narrower-period hint.

Sessions record the sign-in client address and a SHA-256 digest of the User-Agent when available. Authentication audit rows record the client address at sign-in, refusal or explicit sign-out; a sign-out must not reuse an earlier sign-in address. Only a trusted configured ingress may supply forwarded client addresses. Schema version 34 added these fields without reconstructing historical values. Version 35 extends the address to every audited management mutation: the route captures it before the request body is read, the authorization block carries it across the storage mailbox, the storage thread binds it into the staged or mutated row, and the audit trigger copies that column, so replicated statements stay deterministic. Rows the system writes without a request (probe results, notification deliveries, command completion, bootstrap) keep a NULL address, which the Audit page shows as “not recorded”.

25.2. Launch scope (2026-09-11)

The engine of SID 0002 to SID 0006 is the launch-critical product; this console observes and manages it. The project owner closed this record for launch on 2026-09-11 with the scope below. The eight observability

requirements outside that scope were delivered on the same day in phases 1 to 8 of the post-launch plan (see “Post-launch completion”); the launch condition below still applies.

In scope and verified on main: every page of “Pages”, the authentication and kiosk model, the six-topic protocol, the data model through schema version 40, GeoIP, cluster membership, probes and peer telemetry, notifications, retention, response-page templates, the CLI, the build pipeline and digest gate, the golden, contract, end-to-end and cluster test entry points, and the operator guide with screenshots.

Launch condition: the interface and management features are available, but performance acceptance remains separate. The historical paired exception above is not a formal pass and does not cover the updated request path. Fresh October single-node and cross-host matrices are inconclusive; read every new result against the original thresholds and its stated uncertainty before enabling `--console` beside a production data plane. Reproduce a single-node matrix with `zig build console-impact -- --geoip-data <validated-snapshot> --host-label <conditions>`; select `--mode forward_auth` or `--mode reverse_proxy` and repeat with `--capture-heads`. `--cluster` measures three local nodes; the preserved SSH fixture measures separate hosts. Without `--console`, the same binary starts no console thread, listener or sampler.

Accepted deviations: the serve kernel reserves HTTP and control capacity arithmetically (96 slots less 64 browser and 8 peer subscribers), verified by the 64-subscriber scenario, and `libs/serve/src/admission.zig` stays an unwired reference; request bodies use per-route bounded buffers stricter than the 1 MB and 8 MB figures, with policy import chunked; a denial carries no rule name to the client, so tester parity is checked against the decision, not a response header. The interface module has a 768 KiB ceiling and a 640 KiB review threshold since the budget review below. Further page work must pass the asset-size check; changes to the budget require a documented application need and a review of loading and memory costs.

25.3. Post-launch completion (2026-09-11)

Delivered after the launch closure, each with schema, protocol, storage, interface, golden, contract and end-to-end coverage: the client address on every audited management mutation (version 35); revert from the Audit page; active ban entries and nodes-healthy gauges with sixty-second sparklines; durable challenge minutes and their retained window (version 36); resident memory and CPU gauges in the live snapshot and minute records (version 37); sampled referring hosts, client families and response status beside path rankings (SBR2 archives); per-address challenge records and adaptive-difficulty transitions (version 38); and opt-in redacted request and response heads with charset selection and copy-as-cURL (versions 39 and 40, `--console-capture-heads`, `--console-capture-header`). Still open by design: JA4 fingerprints, which the Events detail states as not recorded until a trusted ingress captures them; the solver split on the Challenges page remains self-reported by the client.

Decisions taken in the correctness review that followed (2026-09-11): capture evidence uses a kept-value allowlist rather than a credential denylist, and the response condition is stored with the heads (schema version 40) so absence of a head is never read as a local answer. Challenge-minute summaries page at 32 rows (a full row is 1,792 hex bytes, so 33 rows stay inside the 64 KiB statement envelope) and continue over up to 48 statements per request. The Challenges page states, per booted node, the records dropped by the bounded queue, the batches whose write was not acknowledged, and the difficulty changes observed but not recorded; these counters are boot-local by design, like the minute journals’ unconfirmed snapshots, and are not persisted. The collector ticks every 250 ms and may submit one 32-record batch per tick, so ingestion can reach 128 records per second; each append therefore first removes up to 64 expired records, and the five-second prune of 256 records remains as catch-up, so retention keeps pace at the ingestion bound. The impact runner accepts `--mode reverse_proxy` (against a local origin fixture) and `--capture-heads` (which adds an audited-admission workload); the effective values are part of each result’s provenance.

Acceptance conditions: the impact gate is not formally passed. Current functional evidence is `benchmarks/results/linux-functional-review-20261001.json`: 588 native tests, live console and cluster suites, shipped Wasm behavior, and actual three-host edits, failover, quorum loss, revocation, local commands and clean stops. The connected Chrome walkthrough is recorded in `benchmarks/results/chrome-release-review-20261001.json`, including evidence states, clipboard contents, private policy preview, mobile filters, navigation and the animated connection globe. These checks establish the workflows stated in those records; they do not establish field browser performance or console isolation acceptance. Fresh impact results and their uncertainty must be retained alongside the functional evidence. The interface module measured 622,941 bytes against the 786,432-byte ceiling after the September changes.

25.4. Interface budget review (2026-09-11)

The launch-scope module measured 511,570 bytes against the 524,288-byte ceiling: 370,137 bytes of code, 140,010 bytes of data (about 46 KB of page templates, 40 KB of shorter strings and 52 KB of tables), and under 1.4 KB of ABI metadata (`tools/console_wasm_sections.py` reports the split). The eight observability requirements deferred at launch add panels to the Traffic, Security, Challenges, Events and Nodes pages, which cannot fit in the remaining 2.7 KB. The project owner chose to raise the allocation rather than split the module or reduce existing pages, so the ceiling is 768 KiB and the review warning 640 KiB. Loading evidence for the change: five cold loads of the 511,570-byte module in headless Chrome against a loopback node reached the page heading in 74 to 103 ms (median 98 ms) with a 3 to 6 ms module fetch, so on that path the module cost is instantiation and first render, not transfer; on the 4 Mbit/s planning link a full 768 KiB module takes about 1.57 seconds, which stays within the LCP target only with the immutable cache path (`/console/assets/<digest>/`) serving repeat visits. Linear memory stays at 4 MiB initial and maximum: the module keeps a bump arena reset after each event and fixed buffers, and code size does not change the retained-history bound. Each phase that adds a page records the new module size, and crossing 640 KiB triggers the dependency and browser-timing review above.

26. References

- SID 0002 (foundation architecture), SID 0003 (declarative policy), SID 0004 (semantic inspection), SID 0005 (Zaxonlite storage), SID 0006 (mathematical foundations); repository implementation boundaries are defined in Architecture Overview.
- SID 0010 (the Rust port, which maps the packages named here to Rust crates) and SID 0011 (sqlx storage, which replaces Zaxonlite in the port); cited by the revision note only.
- Krug, Steve. *Don't Make Me Think, Revisited*, 2014; Kahneman, Daniel. *Thinking, Fast and Slow*, 2011. Interface heuristics, not guarantees of operator performance.
- Metwally, A., Agrawal, D., and El Abbadi, A. "Efficient computation of frequent and top-k elements in data streams." *ICDT*, 2005. See also Cormode and Hadjieleftheriou, Finding Frequent Items in Data Streams for Space-Saving bounds.
- zenfmt ZDS 0016, "The zenfmt Server: REST, Streaming, and the Administered Service" (`zenfmt/docs/zds/records/0016-server.typ`, reviewed from the sibling checkout): service, UI/glue and vendored-style patterns. Sibuna defines its own asset build and peer protocol.
- Zig 0.16.0 HTTP/WebSocket source, checked against the installed source; `std.crypto.pwhash.argon2`.
- Tailwind CLI and daisyUI configuration: CLI dependency and explicit component inclusion.
- DB-IP Lite (CC BY 4.0) and MaxMind country CSV schema (provider-specific account, format and licence requirements).
- RFC 6455 (WebSocket), RFC 9110 (HTTP semantics), RFC 6238 (TOTP).
- OWASP password storage and OWASP CSRF prevention.

Lifecycle event

```
2026-10-15: prediscussion -> discussion. Ported from the Zig repository's
Typst record
```

Lifecycle event

```
2026-10-15: discussion -> accepted. State carried over from the Zig
repository's registry
```

Lifecycle event

```
2026-10-15: accepted -> committed. State carried over from the Zig
repository's registry Implemented in the Zig repository; console acceptance
recorded in its SID 0007 review history (2026-10-02)
```