

AIOA AEGIS · BUSINESS-IMPACT-FIRST AIOPS

Business impact first. Decisions backed by evidence.



An AIOps decision platform that puts business impact first

Connects monitoring, assets, topology and operations knowledge into a response process grounded in business context, field evidence and clear ownership.



Chongqing HongChuangDa Technology Co., Ltd.

Business impact

Topology facts

Evidence-based analysis

Private deployment

Product Brochure · v1.4.3 · 2026-09-08

READING GUIDE

From business risk to field evidence

An AIOps decision platform that puts business impact first, connecting infrastructure facts, analysis and coordinated response.

01 IT center heads and executives

See which critical services are affected first, then ownership, progress and verifiable results.

02 Operations and field engineers

Gather evidence from monitoring, assets, topology and skills, with fewer scattered lookups and less re-compiling.

03 Security and technical reviewers

Check permissions, change boundaries, data scope and delivery conditions, and accept against defined scenarios.

Topic	Pages
Business and monitoring	06–07
Onboarding, discovery and topology	08–11
Analysis, assistant and inspection	12–15
Coordination, behavior and governance	16–21
Fit, delivery and feature evidence	22–31

About the screenshots

Screens show the Chinese-language interface. Each caption states whether the data is real, demonstration, simulated or fictional.

BUYING CONTEXT

Problems worth solving in one place

Aegis is for organizations that maintain critical services on an ongoing basis and can provide access to monitoring and devices.

01 Many device alerts, yet business impact is still unclear

Availability probes and business dependencies feed one assessment, instead of everyone guessing from device lists.

02 Assets, monitoring and connections are tracked separately

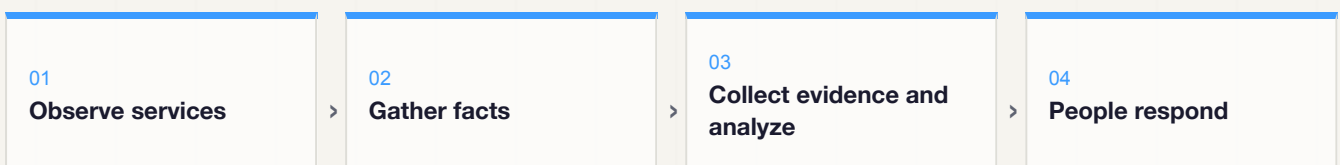
The CMDB organizes onboarding and discovery adds connection facts, so every change has a source and a time.

03 Inspections produce results, but incidents lack a continuous evidence trail

Collection, interpretation, reports and the incident timeline are linked, so whoever takes over can follow the reasoning.

04 Applications look busy, but did the work actually get done?

Access activity and aggregated business results are observed separately, exposing polling and collection blind spots.



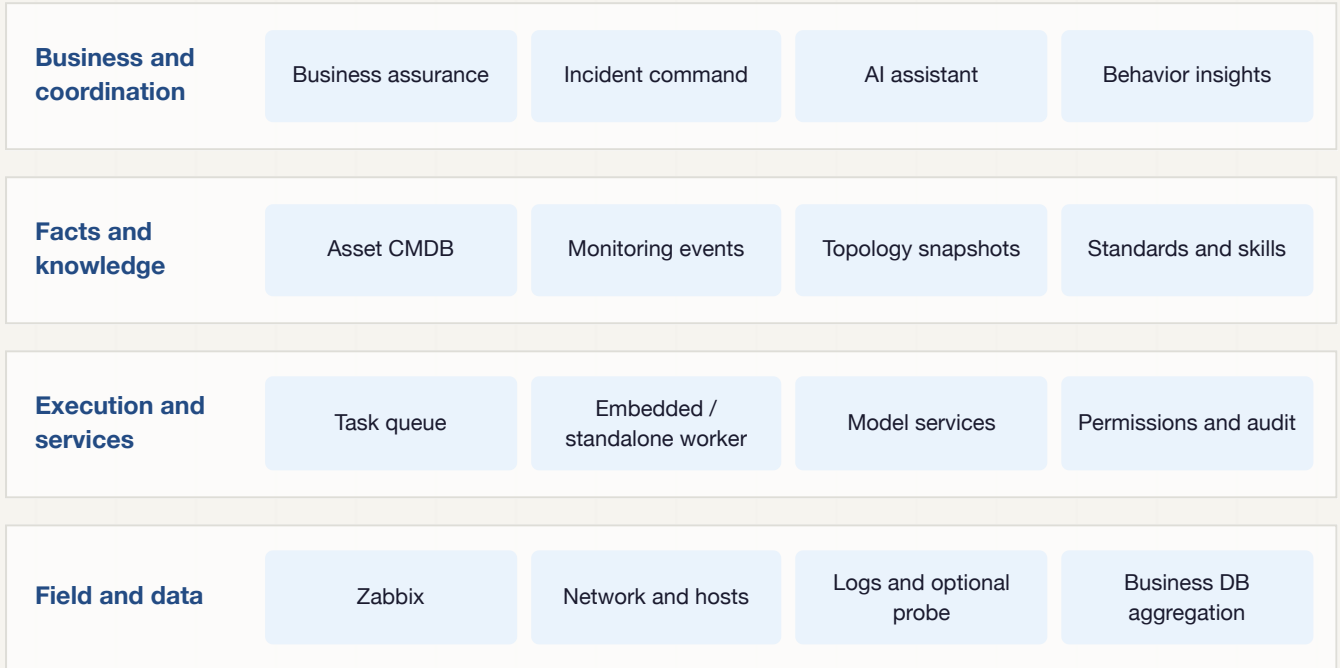
Mechanism diagram · drawn from current feature relationships

Project assessment

For pre-sales validation, choose one well-defined service and a set of authorized assets, and check that inputs, assessments, evidence and response records form a continuous chain.

PRODUCT ARCHITECTURE

One platform, four kinds of work



Layered product diagram · management writes, read-only evidence collection and manual response are authorized separately by function

Business impact sets the priority; assets and topology give location and relationships; skills and models support evidence collection and analysis; coordination workflows keep decisions and accountability with people.

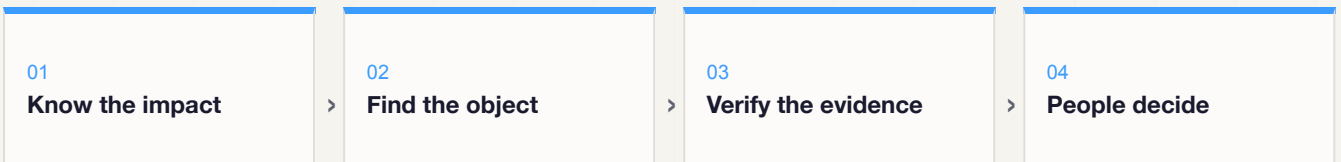
How it fits together

The platform reuses Zabbix monitoring and the customer's model services. Device onboarding, controlled configuration and read-only queries each follow their own permission path.

CORE VALUE

Purchase value, turned into verifiable outcomes

Value	What to verify in the platform
Business impact can be determined	Business tiers, probe results, dependencies and P levels
Infrastructure is traceable	Asset sources, network facts, topology and historical snapshots
Analysis is backed by evidence	Execution transcripts, evidence, conclusions and failure notes
Know-how is governed	Standard items, skill versions, templates and reports
Response ownership is trackable	Incident status, task assignment, timeline and permissions



Mechanism diagram · drawn from current feature relationships

Measuring value

Actual business outcomes depend on models, data coverage, device permissions and on-site processes. This brochure uses no untested accuracy, compression-ratio or time-saving figures.

01 · CORE BUSINESS ASSURANCE

Assess business impact first, then set response priorities

Aegis builds one basis for assessment from business services, availability probes and infrastructure dependencies. Device anomalies are risk signals; business probes directly observe whether a service is available. The two are recorded separately, so a device alert's severity is never taken as the severity of a business incident.

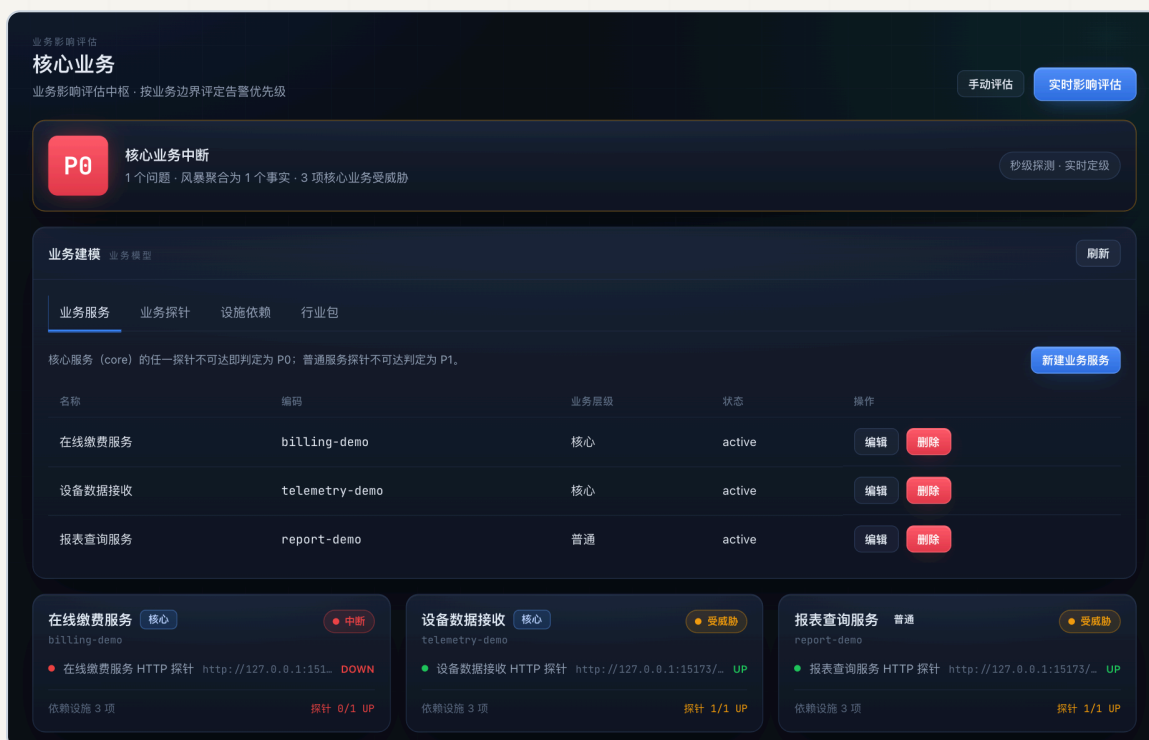


Figure B-01 · Business impact assessment and service status. Real HTTP probes + simulated monitoring (detail)

- Business probes and device anomalies are recorded separately.
- Business tiers and confirmed dependencies together set the scope of assessment.
- Critical services that are already affected are handled first.

Shown in the figure

In the demo, the payment service's HTTP target actually returned 503, producing P0; probes for the other services remained UP.

02 · MONITORING AND EVENT CONVERGENCE

Keep monitoring facts and bring alerts into business context

Zabbix collects device metrics, history and alerts. Aegis reads monitoring status, receives alert events and organizes the live situation view, event convergence and business impact. Each site can link its own monitoring data source.

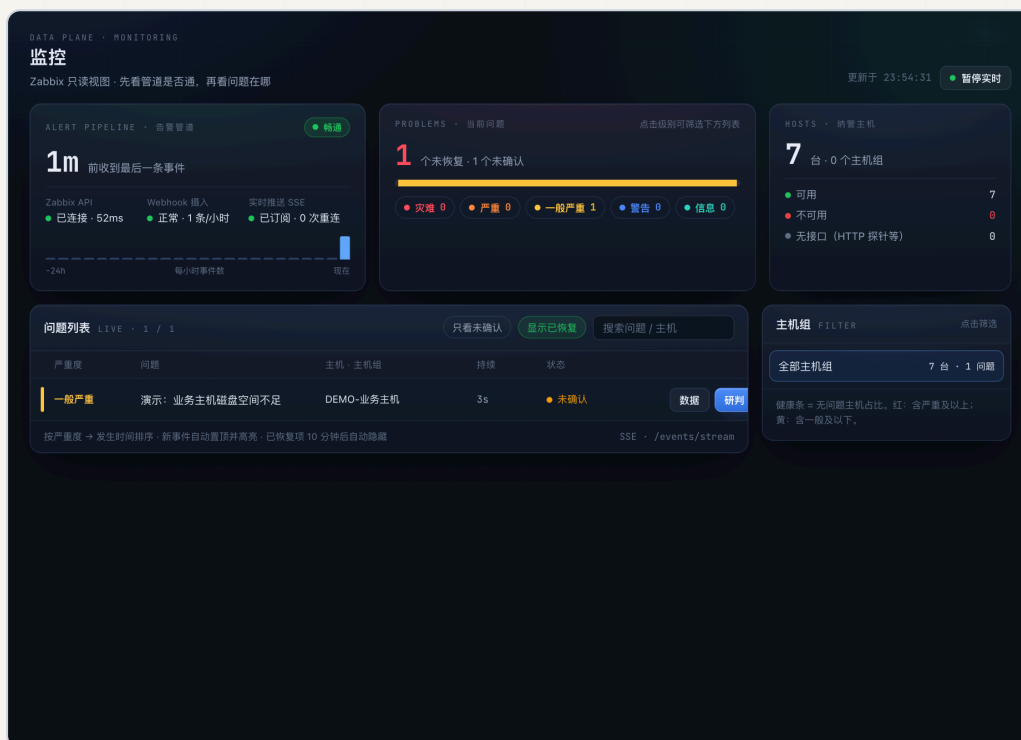


Figure B-02 · Monitoring data pipeline and issue list. Simulated monitoring source · real pages and ingestion path (detail)

- Check the data pipeline first, then the current issues.
- Event sources and update times are retained.
- Move from an issue into metrics and analysis.

Shown in the figure

This example uses a clearly labeled simulated monitoring source; ingestion and the SSE stream are handled by the actual program.

03 · ASSET CMDB AND ONBOARDING

Assets enter the platform, and monitoring configuration follows

Aegis uses the asset CMDB as the management basis for onboarding and synchronization. Customers can take over existing Zabbix hosts or create new assets through device identification; device identity, credentials, classification, tags and monitoring links are maintained in one place.

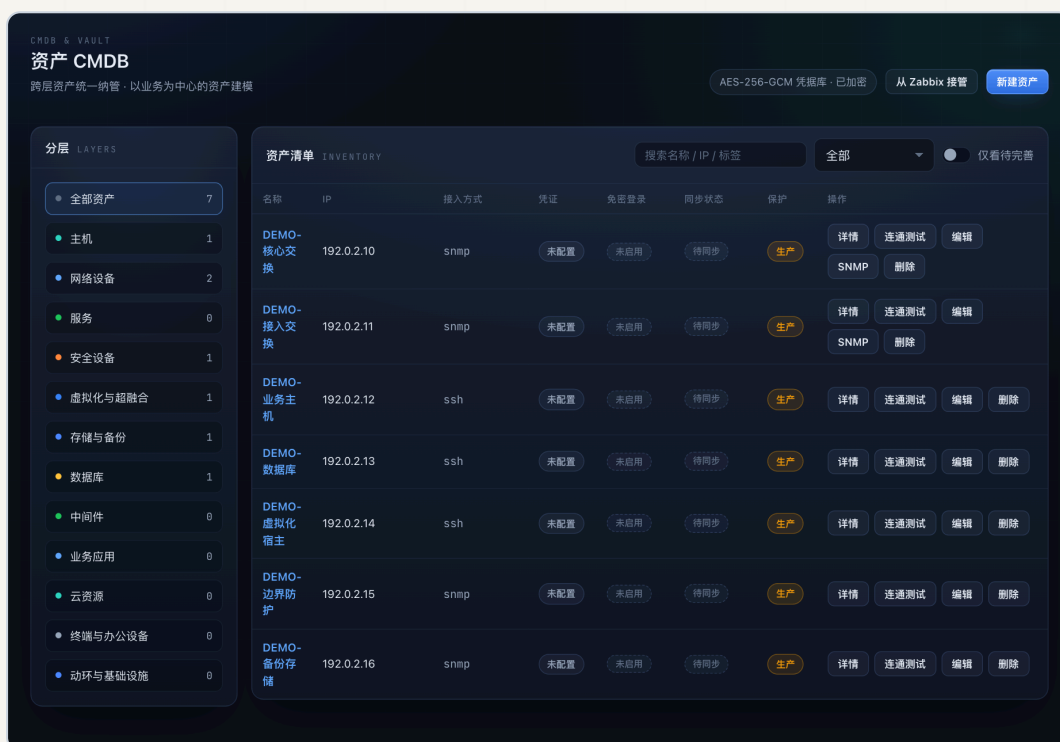


Figure B-03 · Asset list, credentials and sync status. Interface capture · demonstration data (detail)

- Assets are organized by device type.
- Credentials, monitoring links and sync status are checked separately.
- Asset details lead on to facts and history.

Shown in the figure

Addresses and asset names in the figure are fictional examples; credential fields show configuration status only.

04 · CONTROLLED DEVICE CONFIGURATION

Write actions have their own permissions and clear boundaries

Everyday queries, discovery and evidence collection are designed to be read-only; configuration actions that are genuinely needed go through dedicated planning and authorization entry points. Enabling SNMP on a device currently shows a plan first, then asks separately to execute and to save, so configuration changes are never hidden inside diagnostics.

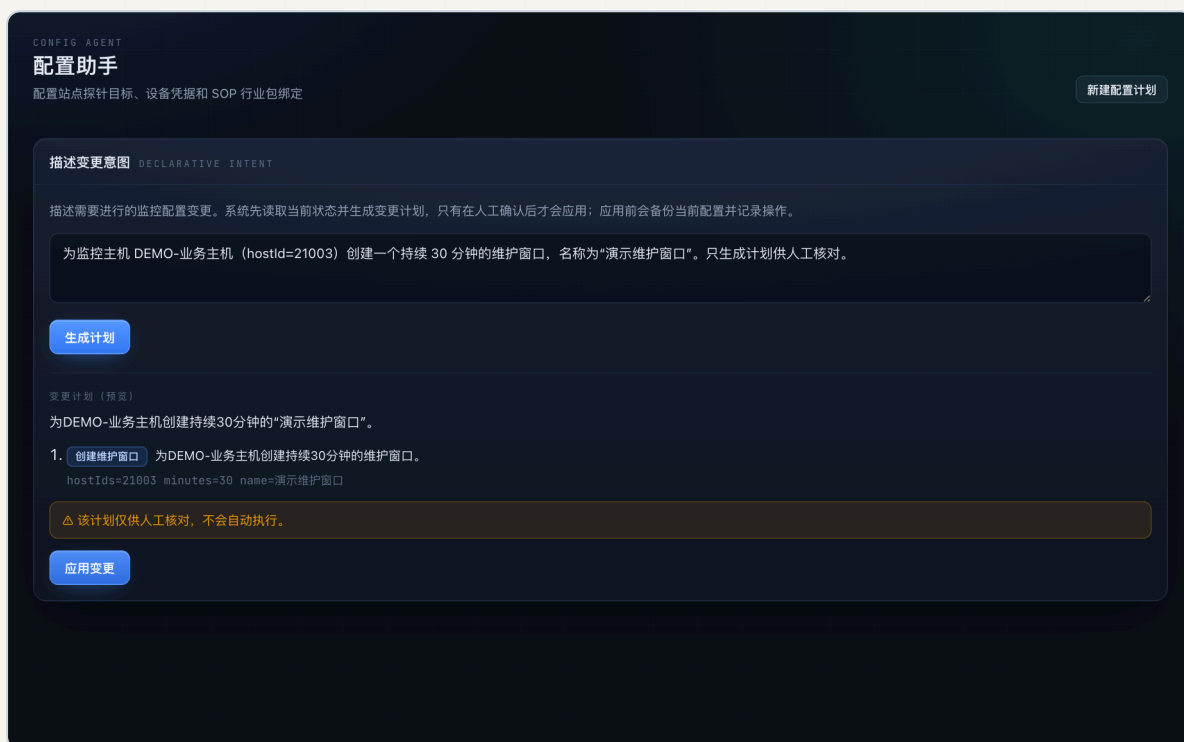


Figure B-04 · Generating a controlled Zabbix change plan. Real plan generation · simulated monitoring object (detail)

- Generate a reviewable plan first.
- Applying changes requires a separate permission.
- SNMP execution and saving are confirmed as separate steps.

Shown in the figure

The real plan identified monitoring host 21003 and proposed a 30-minute demonstration maintenance window.

05 · ASSET DISCOVERY

Keep infrastructure facts complete, within the authorized scope

Discovery starts from switches and their neighbor relationships, reading interfaces, LLDP, ARP, MAC forwarding tables and VLAN information, with optional lightweight endpoint probing configured per scope. Results enter the candidate and fact layers; people then decide what is formally onboarded.

新建范围

名称 *

授权网段 *

多个 CIDR 请用逗号分隔。

192.0.2.0/24, 2001:db8::/64

种子交换机资产

搜索交换机名称或 IP

DEMO-核心交换 · 192.0.2.10

DEMO-接入交换 · 192.0.2.11

SNMP 团体字

探测模式

完整探测 仅 SNMP

探测端口

轻量探测使用的 TCP 端口。以逗号分隔。

22, 23, 80, 443, 161, 3389, 5432, 3306, 1521, 6379, 8080, 10050

最大并发数

每秒数据包数

8 100

定时表达式

可选的五段 cron 表达式；留空表示不定时运行。

0 2 * * *

说明

☒ 启用

取消 保存

Figure B-05 · Setting scope, mode and rate. Configuration form capture

- Declare the scope, seeds, mode and rate.
- Candidates and formal assets are managed separately.
- Incomplete collection does not mean old objects have disappeared.

Shown in the figure

snmp_only and the modes that include endpoint probing must be described separately; discovery currently uses SNMP v2c.

06 · TOPOLOGY AND HISTORICAL SNAPSHOTS

See today's connections, and keep the network as it was during analysis

Interfaces, addresses, open ports, services, links, subnets, VLANs and hosting relationships form structured facts. Aegis builds different topology views from the same facts, and snapshots give incident analysis and change tracing a point-in-time reference.

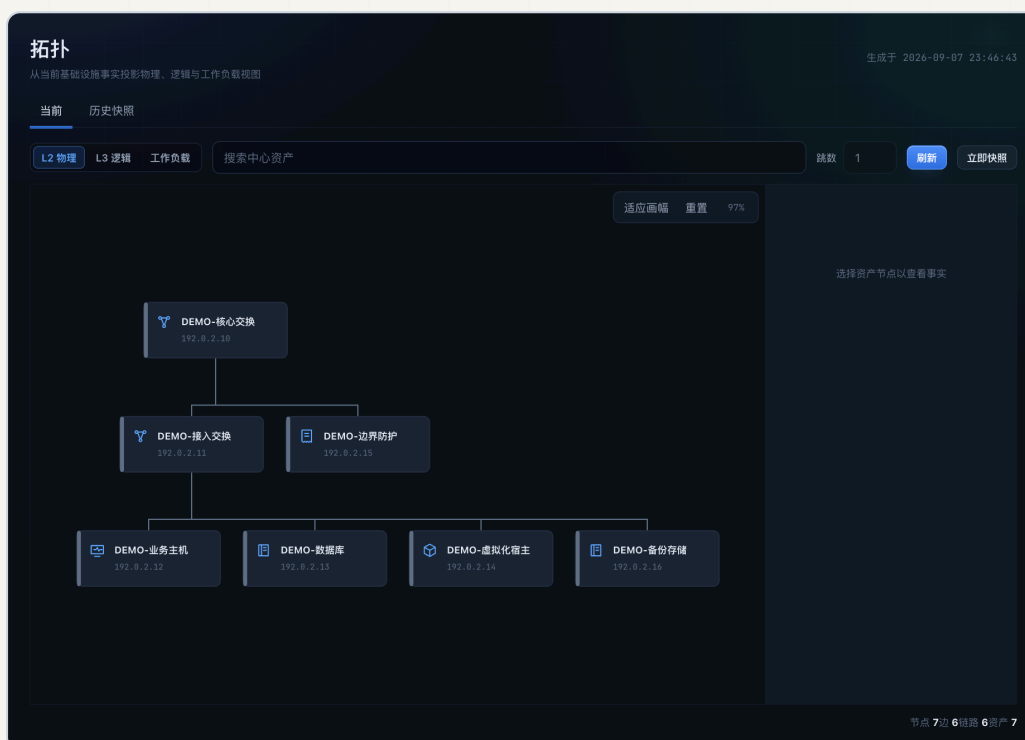


Figure B-06 · L2 physical topology and local relationships. Manually entered topology facts (detail)

- Physical, logical and hosting views share the same facts.
- Topology keeps its source and time.
- Dependency candidates require human confirmation.

Shown in the figure

Seven manually entered demonstration assets and six connections, rendered by the real topology view.

07 · FAULT ANALYSIS AND EVIDENCE

Conclusions trace back to field facts; recommendations go to people

Analysis first organizes monitoring and business impact, then collects field evidence through the selected assets, skills and execution channels. Conclusions contain the judgment, its basis and recommendations, so on-duty staff can review them and coordinate response. Model output alone cannot replace field verification.

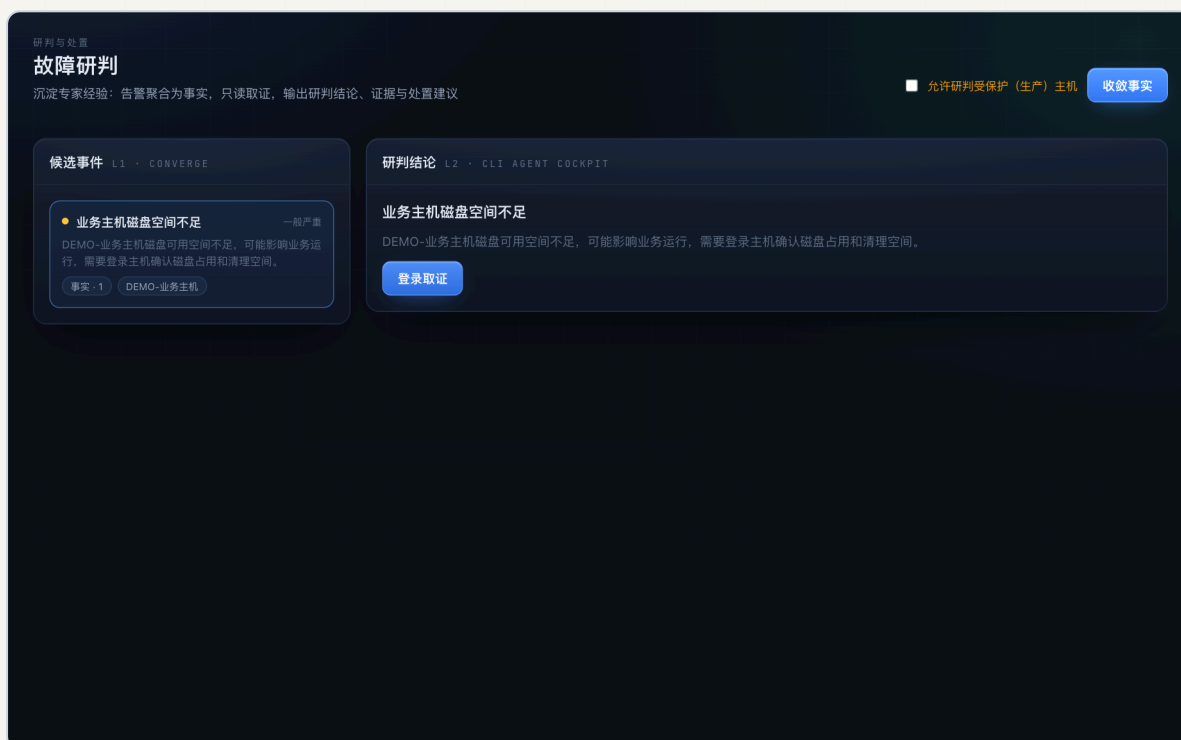


Figure B-07 · From event convergence to a candidate incident. Real model convergence · simulated monitoring input (detail)

- Converge events first, then choose evidence targets.
- Conclusions must map to actual evidence.
- Failures and unknowns are not treated as a fault ruled out.

Shown in the figure

A candidate event produced by real model convergence of a simulated disk alert.

08 · AI OPERATIONS ASSISTANT

Turn facts from many places into answers you can follow up on

The assistant answers questions about assets, monitoring, topology, inspections, analysis, incidents and the knowledge base. Projects and conversations can be organized over time; history is read by the backend per user and conversation, and the current version supports follow-up questions based on successful history.



Figure B-08 · An answer built from platform facts. Real Q&A · demonstration data (detail)

- Answers come from tools the assistant is permitted to use.
- Follow-up questions continue in the same conversation.
- Proposed change drafts are not executed automatically by the platform.

Shown in the figure

A real model answer that distinguishes the already-affected payment service from other services at risk.

09 · STANDARDS LIBRARY AND SKILL CENTER

Turn inspection requirements into maintainable execution knowledge

The standards library holds inspection requirements; the skill center holds vendor, device and channel knowledge. The platform parses documents and assists in extracting check items, injecting matching skills during extraction and execution so that requirements correspond to actual device channels.



Figure B-09 · Reviewing model-extracted check items. Real extraction and review screen

- Clauses, commands and source text can be compared side by side.
- Model-extracted items are reviewed by people.
- Knowledge is maintained continuously per device and channel.

Shown in the figure

The three clauses shown were actually extracted by the model; they are a demonstration specification, not a certified compliance standard.

10 · INSPECTION JOBS AND REPORTS

Collection and interpretation are separate, so evidence can be reused

Inspections organize checks by template, asset scope and executor, and store collection transcripts that the model then interprets into findings and reports. The current version interprets large templates in batches, can keep partial results and, when eligible, re-parses saved evidence only.

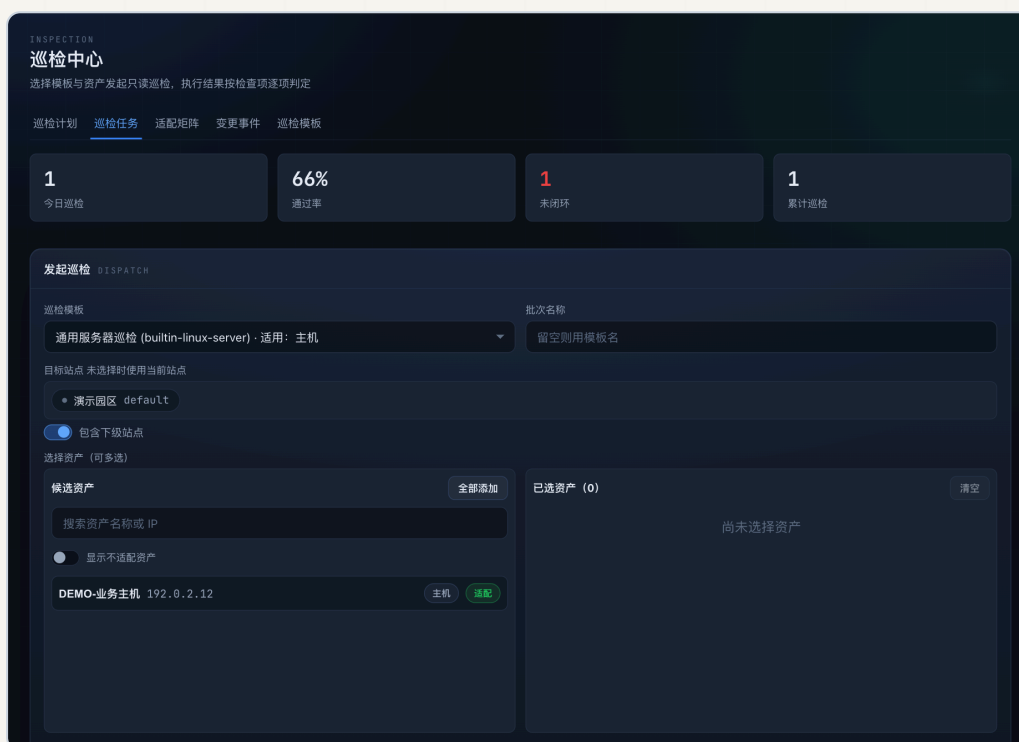


Figure B-10 · Choosing templates and assets: dry run before dispatch. Real job run · isolated container (detail)

- Dry-run the template and asset scope first.
- Collection, interpretation and reporting are staged.
- Results keep failed and undetermined items.

Shown in the figure

Completed demonstration jobs are included in the statistics: three checks produced one failure and two passes.

11 · INCIDENT COMMAND AND COORDINATION

One incident, with clear ownership and progress

Aegis links incidents, task assignment, SLA timers, escalation, notifications and the timeline. On-duty staff collaborate around business impact and field evidence, and authorized people advance each stage, so no finished analysis is left without an owner.

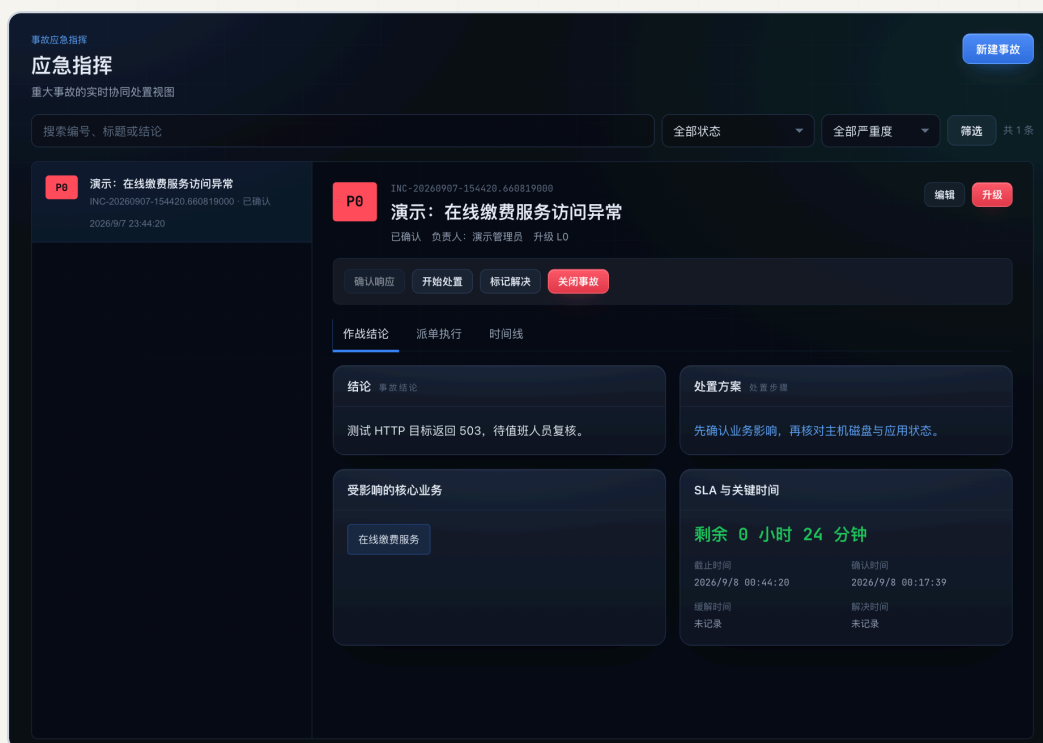


Figure B-11 · Incident status and business impact. Real demonstration incident workflow (detail)

- Incident status and business impact are shown together.
- Tasks state clear instructions and owners.
- The timeline records what was actually done.

Shown in the figure

The demonstration incident has been acknowledged; follow-up handling and closure remain available.

12 · BEHAVIOR INSIGHTS: DATA SOURCES

See access activity and business outcomes separately

Behavior insights ingest gateway logs, an optional browser probe and aggregated business-database metrics. Each source answers a different question (where access happens, how pages are used, whether business operations succeed), and none can stand in for another.

业务数据源 · 演示业务门户

连接业务操作日志库，用于识别网关 HTTP 200 之后的真实业务失败。

☒ 启用业务数据源

数据库主机 * 端口 *

127.0.0.1 25432

数据库名 * 用户名 *

aegis_publication publication_metrics

口令 SSL 模式

留空则不修改 禁用

留空则不修改

数据配置

操作日志

高级

删除数据源 取消 测试连接 保存

Figure B-12 · Business database: fixed mapping and read-only access. Real read-only connection · fictional business logs

- Logs, probe and business database each have their own coverage.
- The business database uses a fixed mapping and a read-only account.
- HTTP success and business success are counted separately.

Shown in the figure

The example connects to a temporary database created for this capture; the account can only query the relevant operation-log table.

13 · BEHAVIOR INSIGHTS: INTERPRETATION AND REPORTS

Fewer misreadings, sounder decisions

A semantic map links paths to business modules, and activity is interpreted against per-application background-polling lists and collection coverage. Zero traffic is classified as unused, unobservable or unmapped, so data gaps are not reported as conclusions about usage.



Figure B-13 · Module heat: comparing usage by business meaning. Fictional logs · real heat statistics

- Go from access activity on to business outcomes.
- Polling and human traffic are interpreted separately.
- Collection blind spots are not reported as idle services.

Shown in the figure

Heat is computed by the actual program from fictional logs. Without an imported menu tree, entry depth is an estimate and should not by itself drive menu changes.

14 · MODEL AND KNOWLEDGE SERVICES

Configure each type of AI call to match the compute you actually have

Aegis manages model services, call bindings, execution engines and OCR presets in one place. Chat, embedding, reranking and image tasks are configured to site capabilities; model IDs can be chosen from the service's current list or entered manually.



Figure B-14 · Binding models by purpose. Settings capture · addresses masked (detail)

- Available models are read per service and key.
- Chat, embedding, reranking and image are bound separately.
- Connectivity and real tasks are verified separately.

Shown in the figure

The chat binding was used for this extraction, Q&A and report; embedding and image were not connected.

15 · PERMISSIONS, CREDENTIALS AND AUDIT

Enforce access scope and operational accountability in the system

The platform organizes access through users, roles, action permissions and site scope, and links management operations to audit records. Asset credentials, executor sessions and model service configuration are managed separately; query, plan, execute and close permissions are split by function.



Figure B-15 · Configuring role permissions by action. Permission settings capture (detail)

- View, edit and execute permissions are granted per action.
- Roles, sites and personal sessions are controlled separately.
- Management operations keep audit records.

Shown in the figure

Permission settings for a read-only role; selections in the interface are not a substitute for full permission testing.

16 · PRIVATE DEPLOYMENT AND OPERATIONS

The center manages facts; execution stays close to the field

Aegis can be deployed as containers or Linux services, with amd64 and arm64 builds. The platform center stores business data and tasks. The embedded executor suits simple deployments; a standalone worker connects outbound to the center to claim tasks and upload artifacts.

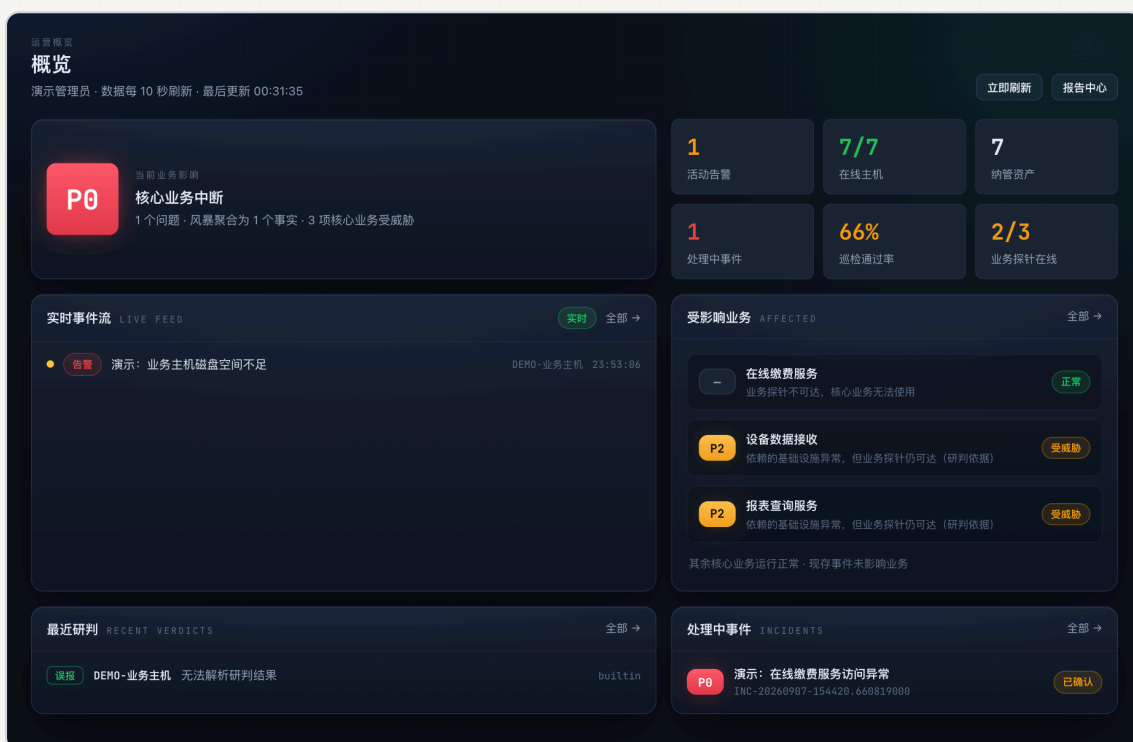


Figure B-16 · Operations overview: from situation to work. Interface capture · demonstration data (detail)

- The center organizes facts, knowledge and tasks.
- Execution sits near the field, depending on the delivery model.
- Versions, permissions and recovery methods are handed over together.

Shown in the figure

The overview is an entry point for navigation and situational awareness; specific judgments rely on each module's sources and timestamps.

SYSTEM INTEGRATION

Connect to existing systems, with clear responsibilities

System or component	Responsibility	How Aegis connects
Zabbix	Metrics, history and monitoring alerts	Site data sources, onboarding sync, event and impact views
Model services	Text inference, embeddings and similar capabilities	Per-task binding, connectivity tests and run records
Devices and executors	Field access, commands and APIs	Asset credentials, skills, workers and evidence upload
Business applications	Gateway logs, page events, operation results	Behavior attribution, polling tiers and aggregated reports

Every integration point must answer three questions: what can be read, what may be changed, and how failures are recognized. The clearer the responsibilities between systems, the easier delivery results are to check.

Scope

The platform database is PostgreSQL. The business-database aggregation source is a separate external connection and is not a compatibility commitment for the main database.

Three responsibilities to settle at integration

- Data: who maintains monitoring, assets, business models and semantic mappings.
- Permissions: who issues read-only access, and who approves necessary management writes.
- Recovery: who checks status and restores service when a data source, model or executor is unavailable.

PROJECT FIT

Good-fit projects have clear business boundaries

Critical service continuity

IT centers that want to link device anomalies, service availability and response priority.

Multi-site daily operations

Sites manage their own facts, executors sit near the field, and the center organizes tasks.

Standardized inspection

Existing inspection requirements that need continuous management of templates, skills, evidence and reports.

Application operations review

Teams that want to tell real business use apart from background polling, and see transaction outcomes.

Prerequisites for a project

- Critical services and probe coverage are defined, and confirmed dependencies can be maintained.
- Controlled monitoring access, read-only device accounts and model services are provided.
- Write approvals, division of responsibility, data scope and the acceptance environment are defined.

Scope

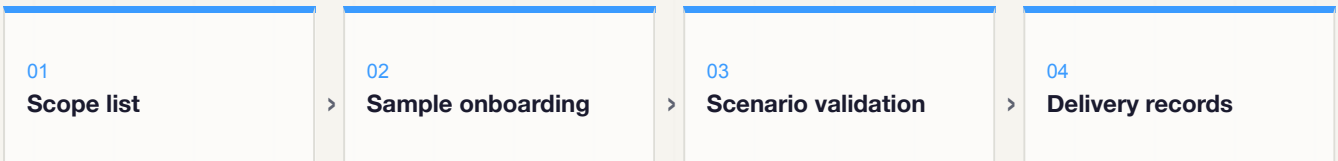
Purchasing this version does not presuppose unattended self-healing, full network traffic analysis, unlimited scale or general-purpose database replacement.

DELIVERY METHOD

From small-scale validation to formal delivery

Build trust with a sample that can be verified repeatedly, then expand to the site's full scope.

- 01 Confirm scope: list sites, assets, critical services, models, interfaces and any required change permissions.
- 02 Establish facts: take over or onboard sample assets first, then complete probes, dependencies, discovery scope and skills.
- 03 Validate the loop: use controlled anomalies to verify impact, evidence, tasks and reports; test failure and recovery separately.
- 04 Deliver and archive: record versions, configuration, permissions, templates, backup and recovery, and acceptance.



Mechanism diagram · drawn from current feature relationships

Scope

Each phase is defined per project. The illustrative flow is not a promise of go-live within a fixed number of days, or of delivery without tuning.

ACCEPTANCE FOCUS

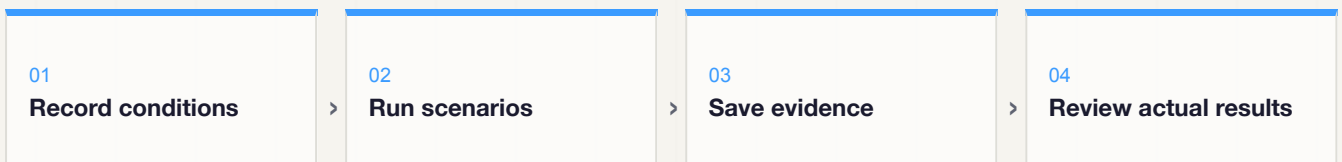
Acceptance examines the process, including how failures are handled

Topic	Records to keep
Business impact	Probe changes, P levels, and the difference between infrastructure risk and business impact
Discovery and topology	Authorized scope, partial collection, candidates, snapshots and differences
Assistant and permissions	Follow-up records, tool permissions, separation of drafts from execution
Inspection recovery	Collected evidence, undetermined items, re-parse-only results
Behavior insights	Sources, mappings, polling, dormancy reasons and business aggregation
Delivery and recovery	Versions, worker uploads, backup and restore results

Acceptance should use isolated or explicitly approved test objects, with the customer and the delivery team jointly recording conditions, operations, and expected and actual results.

Evidence basis

This brochure describes product capabilities and how to verify them. Preparing these materials is not presented as customer on-site acceptance.



Mechanism diagram · drawn from current feature relationships

RELEASE NOTES

v1.4.3: capability update based on the current code

01 Business and delivery foundations

A maintainable business model, incident coordination, standalone worker and private deployment are in place.

02 Assets and topology

CMDB onboarding sync, controlled SNMP configuration, discovery facts, topology snapshots and dependency candidates are covered in this edition.

03 Models and execution

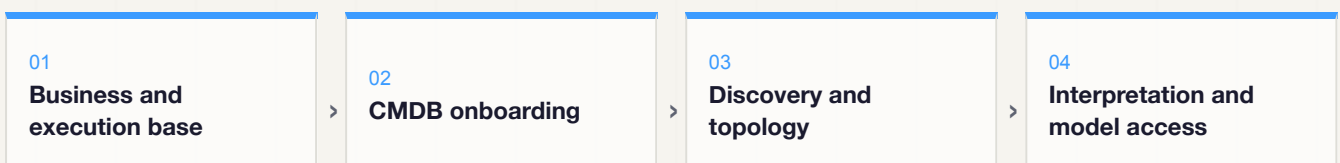
Large-document extraction, channel matching, batched inspection interpretation and re-parsing, and model lists read per service.

04 Latest local increments

Conversation history and change drafts; business-database aggregation, full semantic-map import, per-application polling and probe delivery.

Version baseline

Product version v1.4.3; source verified up to 2eedaf0 (2026-09-04). Local commits include later improvements under the same version number; the actual delivery package is identified by its build commit.



Capability evolution diagram · actual delivery is still verified against the build commit

COLLABORATION VALUE

Managers, operations and security working from the same facts

Managers

Confirm priorities by business impact, and follow response progress and report conclusions.

Operations staff

Gather evidence through assets, topology and skills, drive tasks and feed back experience.

Security staff

Review device permissions, change plans, credentials and data-flow boundaries.

Delivery staff

Define versions, components, scope and recovery methods, and prove delivery with scenario records.

01

Business model

>

02

Field evidence

>

03

Clear ownership

>

04

Continuous review

Mechanism diagram · drawn from current feature relationships

Aegis provides a shared foundation for information and collaboration. Whether a service has recovered, whether a configuration may change and whether an incident is closed are still decided by authorized people, based on the facts.

FEATURE EVIDENCE

One real inspection, with evidence for every item

Three checks on an isolated container ran end to end through the product; each result can be checked against the raw output.



Figure B-17 · Per-item verdicts and execution evidence. Real read-only collection and model interpretation

- Disk usage of 95% exceeded the demonstration threshold and was judged a failure.
- The memory field and UTC time checks passed.
- No cleanup, restart or configuration change was performed.

Image source

Real read-only collection and model interpretation

FEATURE EVIDENCE

Inspection results flow into the native delivery report

Reports organize chapters by inspection content; generation status, body text and optional outputs are each visible.

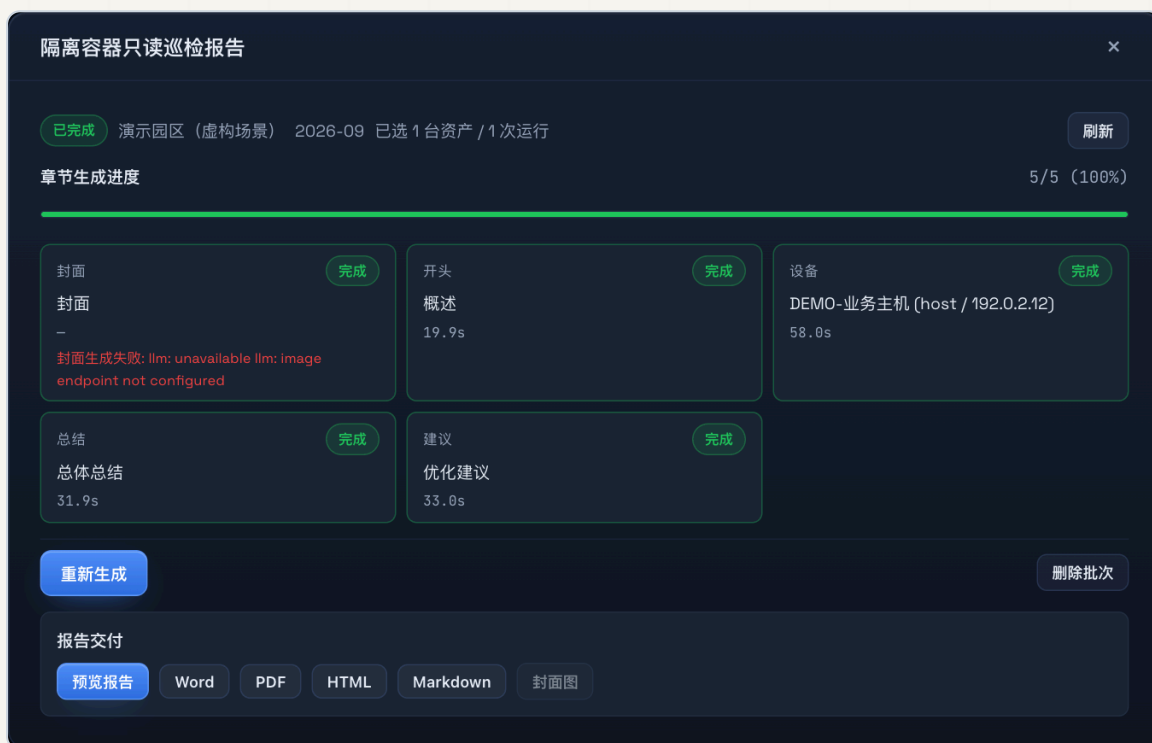


Figure B-18 · Viewing chapter progress and export status. Native product report · actual generated result

- In this example the body was generated, with working preview and export entry points.
- No cover image was configured; the interface keeps the corresponding notice.
- Before external use, delivery staff check the scope and conclusions.

Image source

Native product report · actual generated result

FEATURE EVIDENCE

Beyond HTTP: see whether the business transaction succeeded

Business-database aggregation adds operation outcomes that access logs cannot see, giving application reviews another set of facts.



Figure B-19 · Business action failure analysis. Fictional business data · real aggregation

- The statistics shown come from fictional business logs in a temporary database.
- Successes and failures are broken down by business action.
- Only aggregates are shown: operation count, failure rate and number of participants.

Image source

Fictional business data · real aggregation

FEATURE EVIDENCE

Separate collection blind spots from idle services

Zero traffic can have entirely different causes. First explain what the data can see, then discuss business use.

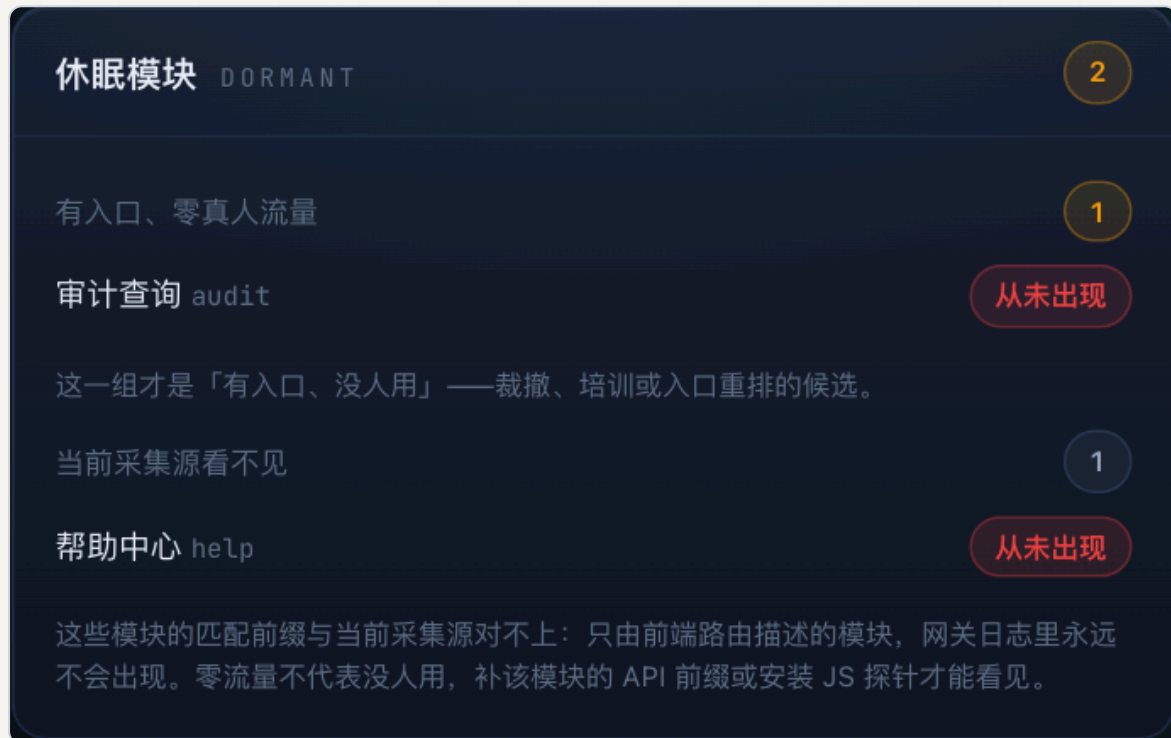


Figure B-20 · Module heat and dormancy reasons. Fictional logs · real reason classification

- Audit query: no human traffic was observed in this window.
- Help center: not observable from the current source.
- Check mappings and collection coverage before drawing business conclusions.

Image source

Fictional logs · real reason classification

AIOA AEGIS · BUSINESS-IMPACT-FIRST AIOPS

Start from business impact. Deliver verifiable results.



Business assurance · Field evidence ·
Knowledge governance · Coordinated response

Build a reviewable foundation for operations decisions around your critical
services, existing monitoring and delivery scope.



Chongqing HongChuangDa Technology Co., Ltd.

www.cqagc.com

Business impact

Topology facts

Evidence-based analysis

Private deployment

Product Brochure · v1.4.3 · 2026-09-08