

Recover the Hermes Agent connector

Use this runbook when a Hermes Agent host is unavailable, not ready, losing its lease, rejecting traffic, or retaining work whose provider outcome is uncertain. It helps you locate the failing boundary and recover the same AIP Action, opera

SECTION	Connectors
TYPE	Connector
PROTOCOL	AIP 1.0
SOURCE	docs/connectors/hermes-agent/operations/health-observability-and-recovery.md

Run these checks through an operator-controlled network. The procedure assumes the fixed endpoint set and shared PostgreSQL boundary established in [Deploy the Hermes Agent connector](#).

Contain risk before diagnosis

Pause new model, tool, session, job, operator, and delegation mutations for the affected binding when durable storage is unavailable, the host lease is invalid, or an accepted operation has an unknown outcome. Keep bounded reads available only when tenant and endpoint ownership remain verified.

Do not restart Hermes, clear either database, rotate an endpoint, create a new Action ID, or move pinned work as the first response. Retain:

- UTC incident start and the last known-ready time;
- connector type, version, instance, replica, artifact, and manifest digest;
- tenant, endpoint ID, provider origin, configuration, and credential revision;
- lease sequence, lease expiry, and registry status;
- Action, idempotency, correlation, session, approval, delegation, and run IDs;
- `/ready` plus two timestamped `/metrics` snapshots;
- AIP results, events, chunks, receipts, and redacted provider evidence;
- operator binding status and provider job or session identity when relevant.

A healthy replacement cannot make an earlier uncertain model or tool effect safe to repeat.

Read six views in order

No single surface proves the outcome of an Action.

View	What it answers	What it does not prove
Host <code>/health</code>	Can the common host process answer its static route?	Lease, storage, endpoint, or provider readiness
Host <code>/ready</code>	Are drain, lease, PostgreSQL, and all basic endpoint probes ready now?	Bearer auth, model credentials, MCP, tools, or one Action outcome
Host <code>/metrics</code>	Are local load, rejection, heartbeat, and lease signals changing?	Per-endpoint, per-capability, or per-Action truth
Registry and gateway	Is the replica eligible and where is accepted work pinned?	Whether Hermes or a tool committed an effect

View	What it answers	What it does not prove
Protected Hermes read	Does the selected endpoint accept its Bearer token and expose the expected model or runtime view?	Chat, tool, mutation, or delegation success
AIP and provider state	What evidence belongs to this exact Action and provider handle?	General readiness for new work

Capture the host surfaces without submitting an Action:

```
SH
export HERMES_HOST_OBSERVE_ORIGIN=https://hermes-connector.internal.example

curl --silent --show-error "$HERMES_HOST_OBSERVE_ORIGIN/health"
curl --silent --show-error \
  --write-out '\nHTTP %{http_code}\n' \
  "$HERMES_HOST_OBSERVE_ORIGIN/ready"
curl --silent --show-error "$HERMES_HOST_OBSERVE_ORIGIN/metrics"
```

Do not expose these unauthenticated host routes to an untrusted network. Scraping `/metrics` does not exercise the endpoint Bearer token.

Interpret host readiness precisely

`/health` returns static process metadata. `/ready` returns HTTP 200 only when all four gates pass and HTTP 503 otherwise:

Readiness field	Ready value	Failure boundary
<code>draining</code>	<code>false</code>	Planned or interrupted shutdown
<code>lease_valid</code>	<code>true</code>	Lifecycle network, registry, clock, or expired lease
<code>runtime.ready</code>	<code>true</code>	PostgreSQL read/write readiness
<code>connector.ready</code>	<code>true</code>	Basic health of every configured Hermes endpoint

The response includes `runtime.durability` and a startup recovery summary:

Recovery field	Meaning
<code>recovered_at</code>	Time at which startup recovery began
<code>pending_approvals</code>	Existing approvals retained for continuation
<code>recoverable_transactions</code>	Transactions retained for reconciliation
<code>queued_results</code>	Queued Actions completed during startup recovery
<code>delegation_results</code>	Delegations completed during startup recovery
<code>callback_deliveries</code>	Callback deliveries resumed during recovery

This summary is startup evidence, not a live backlog. A queued-action or delegation recovery error blocks registration. A broader storage or callback recovery failure also stops host construction instead of producing readiness.

Connector readiness visits every endpoint in normalized endpoint order and sends unauthenticated `GET /health`. Every endpoint must return parsable JSON with a successful HTTP status. The readiness loop does not require the JSON `status` field to equal `ok`.

The configured host health timeout wraps the complete multi-endpoint loop. Its default is 2000 milliseconds, even though one direct endpoint health request has a 30-second client timeout. A slow first endpoint can therefore end the whole host probe before later endpoints are visited.

Basic endpoint health does not prove Bearer authentication, model-provider credentials, MCP connectivity, tool availability, or operator policy. Confirm the intended endpoint with the authenticated `health_detailed` or `models` capability after host readiness returns.

Interpret the eight host metrics

The host emits exactly eight unlabeled Prometheus metrics:

Metric	Operational use	Important limit
<code>aip_connector_host_ready</code>	Combined lease, drain, storage, and connector state	Uses cached probe flags; correlate with <code>/ready</code> and registry state
<code>aip_connector_host_storage_ready</code>	Last durable-storage probe result	Does not identify a damaged record
<code>aip_connector_host_in_flight</code>	Actions executing in this process	Does not include provider work after a lost response
<code>aip_connector_host_requests_total</code>	Native messages observed by the host	Does not count every HTTP request or classify capability success
<code>aip_connector_host_rejected_total</code>	Native messages rejected before successful handling	Requires signed error-code correlation
<code>aip_connector_host_heartbeat_failures_total</code>	Failed renewal or lease-recovery cycles	One increase does not prove lease expiry
<code>aip_connector_host_lease_recovery_attempts_total</code>	Re-registration attempts after lease expiry	Includes attempts that did not recover
<code>aip_connector_host_lease_recoveries_total</code>	Successful expired-lease recoveries	Does not resolve Action or provider outcomes

The metrics endpoint returns HTTP 200 even when the ready gauge is 0. Storage and connector gauges are refreshed by readiness checks and heartbeat probes, not by a new probe inside each metrics scrape. Counters and gauges are process-local and reset when the host restarts.

This revision exposes no Hermes endpoint label, provider status, latency, model, MCP, run, approval, session, job, operator, or delegated-result metric. Use durable AIP records and bounded provider reads for those views.

Define alert windows from the deployment SLO. At minimum, alert on these relationships:

- readiness remains 0 outside a planned drain;
- storage readiness remains 0 or `/ready` reports storage failure;
- heartbeat failures grow as the current lease approaches expiry;
- lease-recovery attempts grow without a successful recovery;
- in-flight work remains at the configured concurrency bound;
- rejected messages grow faster than total native messages;
- basic endpoint health passes while a protected read fails;
- an accepted Action stops producing durable state within its contract bound.

Classify the failing boundary

Observation	Boundary	Immediate decision
No host response	Process, node, ingress, or network	Preserve both state stores and follow hard-crash recovery
/health works and draining is true	Planned or partial shutdown	Stop new assignments and finish or investigate the drain
lease_valid is false	Lifecycle TLS, DID, clock, registry, or admission	Keep mutations paused and allow fenced recovery after repair
runtime.ready is false	Connector PostgreSQL	Isolate the replica; never substitute an empty database
connector.ready is false	One or more endpoint origins or basic health routes	Restore every endpoint or revise the admitted endpoint set
Host ready, protected read gets 401 or 403	Endpoint token or endpoint selection	Replace the correct token and host process
Host ready, models read fails	Model provider, route alias, quota, or credential	Keep model and tool work paused; basic health is insufficient
Rejections rise with high in-flight work	Local capacity	Preserve Action IDs and let bounded backpressure work
Rejections rise with low load	Schema, signature, route, policy, credential revision, or execution	Group by exact signed error code
Bound operator run cannot be found	Hermes provider run state	Reconcile as volatile provider-state loss; do not start again
Queue and lifecycle disagree on a delegated result	Durable integrity	Fail closed and preserve both records

Recover process or lease loss

If the host still runs, repair lifecycle DNS, TLS, CA trust, pinned DID, clock, or service availability before replacing it. The host retains its last lease until expiry. While the lease is valid, each heartbeat reports the combined storage and connector result. An unhealthy report moves the replica offline.

After lease expiry, a healthy host uses signed re-registration instead of a heartbeat. An ambiguous lifecycle response is retried with the same request identity and registration bytes. A definite admission or configuration rejection clears that request; correct the immutable mismatch before the next attempt. Never edit lease expiry, sequence, or registry status by hand.

After a hard crash:

1. prove that no process still owns the replica key and endpoint;
2. preserve the same PostgreSQL database, artifact, instance, and replica;
3. preserve each Hermes endpoint's local state and provider identity;
4. wait for clean offline state or lease expiry;
5. start the reviewed process and let recovery finish before registration;
6. stop if recovery reports queued-action or delegation errors;
7. compare recovery counts, retained assignments, and the new lease sequence;
8. require host readiness and one protected read before restoring traffic.

Use a new replica identity for an actual replacement. Never run two processes with the same replica ID or signing key, and never point overlapping replicas at independent connector databases.

Recover storage, endpoints, and capacity

When `runtime.ready` is false, restore connectivity to the exact PostgreSQL database. Check capacity, certificates, role permissions, schema, and read/write health. Do not initialize a clean store; that removes the state needed to fence Actions, approvals, callbacks, operator bindings, and child results.

When `connector.ready` is false, identify the failing endpoint from the bounded connector detail and endpoint evidence. Check its fixed origin, network trust, Hermes process, and JSON health response. One failed endpoint keeps the complete host unready. Restore it or change the endpoint set through the reviewed deployment and admission process.

A protected read failure requires separate checks for endpoint ID, Bearer token, Hermes API-server policy, model route, and upstream credentials. Replacing token bytes requires a host restart because endpoint keys are read at startup.

At local capacity, a new Action receives retryable `connector_host.capacity` with HTTP 429. A draining, lease-invalid, or connector-unready host returns retryable `connector_host.not_ready`. Preserve the original Action contract and honor backoff. A retryable transport label does not prove that Hermes or a tool performed no work.

Recover by provider state owner

First read the durable AIP Action, including its result, events, chunks, approval, and delegation links. Then use the operation's provider-owned state:

Work family	Provider state at the pinned revision	Recovery decision
Health and discovery reads	Point-in-time endpoint response	Repeat only as a new governed read when the original Action is settled
Chat and Responses execution	Model and tool work may already have started	Read the original AIP result first; do not resubmit automatically after transport, decode, deadline, or server failure
Stored Responses objects	Normally endpoint-local SQLite; may fall back to memory if that store cannot open	Read by the retained response ID on the owning endpoint; absence does not authorize model replay
Structured runs	Status, stream queue, active task, and approval session are in process memory	A provider restart can lose the <code>run_id</code> ; preserve AIP evidence and do not recreate the run
Persistent sessions	Endpoint-local <code>state.db</code> ; no in-memory session fallback	Read the session and messages on the owning endpoint before repeating create, patch, fork, chat, or delete
Scheduled jobs	Profile-local persistent scheduler files and run claims	Read the current job and output evidence; an accepted mutation does not prove a due run or delivery
Operator execution	Durable PostgreSQL binding plus a volatile provider run	Resume observation only when a bound <code>run_id</code> still exists; otherwise preserve the uncertain outcome
Delegated child	Exact durable queue and lifecycle records	Accept only a matching terminal result for the expected child Action and principal

Endpoint identity includes its local Hermes home and runtime state. Do not redirect an existing endpoint ID to an empty Hermes instance and treat a missing response, session, job, or run as proof that no effect occurred.

Recover an operator or delegated result

The standalone host stores operator bindings in the same PostgreSQL-backed profile state used by its runtime. Each binding retains the source Action, endpoint, request fingerprint, provider run ID when known, cancellation intent, approval generation and commands, sequence, terminal output, and typed error.

Use this decision order:

1. read the source Action and retained operator binding;
2. reject any endpoint or request-fingerprint mismatch;
3. return a retained terminal result without contacting Hermes again;
4. when `run_id` is bound, poll that exact run and reconcile cancellation;
5. when start ownership disappeared before `run_id` was stored, keep `outcome_unknown` and do not replay `POST /v1/runs`;
6. when an approval command is claimed without a durable outcome, preserve its uncertain state instead of sending the choice again;
7. require a Hermes terminal status before calling cancellation confirmed.

A provider `404` for a bound run can mean provider restart or retention loss. It does not prove that models or tools had no effect.

For first-class delegation, the resolver reads the exact child Action from the durable queue and lifecycle stores. It verifies child identity, tenant, transport-authenticated Hermes principal, and immutable execution contract. A terminal record without a result, conflicting queue and lifecycle results, or a missing expected child is an integrity or policy failure. Never substitute the Hermes model's final prose for that result.

Preserve stream and event evidence

AIP Action events and chunks use durable runtime positions. Persist the opaque combined cursor only after processing its page. Provider SSE event IDs, provider run IDs, chunk IDs, and AIP cursors are not interchangeable.

A lost follow connection does not cancel an Action. Initial operator observation can consume the volatile Hermes SSE queue; after reconnect or host restart, a bound operator polls provider run status instead. Chunks already published to AIP remain available, but unobserved provider events may be lost.

Do not infer terminal execution from an ended stream. Require the durable AIP result and, where applicable, the provider's terminal state.

Verify recovery

Restore affected traffic only when every applicable check passes:

1. `/health` and `/ready` agree on a live, non-draining host;
2. storage and all endpoint probes are ready within the configured bound;
3. the registry shows the intended replica with a current lease;
4. metric growth has stabilized and usable capacity remains;
5. one protected read reaches the intended endpoint and credential;
6. each retained Action has a justified durable state under its original ID;
7. provider-local sessions, jobs, responses, and runs are read from their owning endpoint rather than inferred from host readiness;
8. uncertain operator, approval, cancellation, or tool effects remain paused until terminal evidence exists;
9. the incident record retains identities, state transitions, errors, and operator decisions.

If these views disagree, keep the mutation boundary paused. Escalate with the source revisions, artifact and manifest digests, endpoint set, database identities, lease history, readiness body, metric snapshots, Action and provider identifiers, operator binding, and redacted evidence.

Related documentation

- [Deploy the Hermes Agent connector](#)
- [Operate the connector host lifecycle](#)
- [Observe and recover AIP work](#)
- [Run a governed Hermes operator lifecycle](#)
- [Errors and retry decisions](#)