



HANDS-ON WALKTHROUGH · CRIBL STREAM

Is your Cribl Stream deployment healthy?

One tenant watches a Cribl Stream deployment end to end — its Sources, Destinations, Pipelines, Routes, Workers and Leader — from the metrics Cribl already sends to Splunk and from its Leader API, and tells you, in a Cribl operator's words, what needs attention.

Captured live on TrackMe 2.4.19 · Cribl.Cloud and self-managed lab deployments



Every object in the data path is a place where data can stop

Cribl shows you the state of the moment. Someone has to keep watching it — every Destination, every Route, every Worker, every hour.

Destinations under pressure

A Destination in backpressure or blocked, events dropped, a Source reported unhealthy: the data is late or lost before anyone looks.

Traffic that changes shape

A Source sending half of what it usually sends at this hour, a Route that goes quiet: nothing is broken, the volume is just wrong.

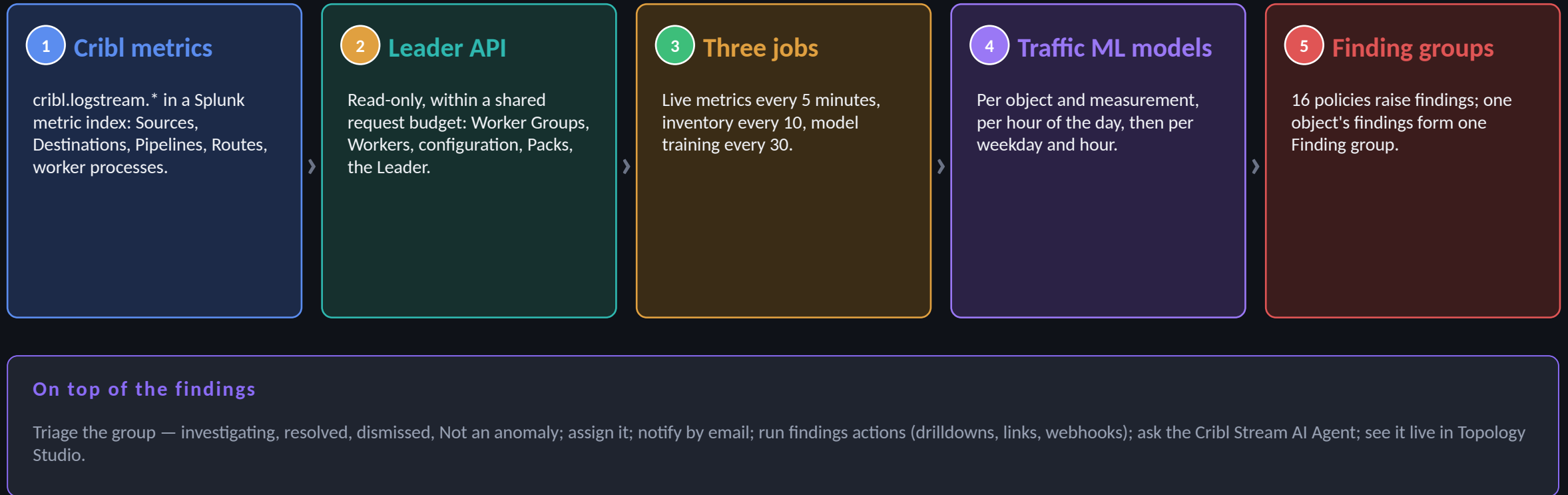
Workers that drift

A Worker that stopped answering, runs another version than the Leader, or an old configuration; a Leader whose disk is filling up.

What a Cribl Stream tenant does

A dedicated tenant type. It reads the Cribl internal metrics your Workers already send to a Splunk metric index — in place, nothing copied — and the Cribl Leader API, read-only within a shared request budget. Sixteen built-in policies raise findings, a traffic ML model learns the normal traffic of every object and every hour, and a purpose-built workspace gives the investigation and triage workflow. TrackMe never changes anything in Cribl.

Two sources you already have, three jobs, findings you can act on



A dedicated tenant type: no entities, no decision maker, no health score. Its objects are Cribl objects; one tenant per Cribl connection.

What we are going to do — one tenant, four parts

PART 1

Setup

- A Cribl connection
- The creation wizard
- The tenant card and the strip
- Collection health, day one

PART 2

Findings

- The Findings tab
- Finding groups and triage
- Investigating an outlier
- Assignment and webhooks

PART 3

Observe

- Traffic and resources
- Traffic ML models and tuning
- Workers and the Leader
- Routes, pipelines, flows

PART 4

Operate

- Inventory and exclusions
- Policies and notifications
- The AI Agent and assistant
- Topology Studio, Guardian

Every screen is the product as shipped, on lab deployments with real traffic.

01

PART 1 • SETUP

Connect, create, collect

A Cribl connection declared once, the four-step creation wizard, and the first collection: the tenant card, the status strip and Collection health on day one.

A Cribl connection — declared once, read-only

Manage Cribl connections

Create, edit and test Cribl Cloud or self-managed connections. Credentials are stored encrypted in Splunk. Requires administrator access and an Enterprise or Unlimited license.

[Cribl connection alerts in Configuration Guardian](#)

2 connections · 2 enabled · 0 disabled. Tests run sequentially and skip disabled connections.

CONNECTION	DEPLOYMENT / SCOPE	STATE	CONNECTIVITY	LAST CHECKED	ACTIONS
cribl_cloud	Cribl Cloud example-org / main Leader budget: 1,200 requests per hour, burst 150 Certificate verified	Enabled	Connected	12/10/2026, 13:48:29	
cribl_trackme_docker	Self-managed https://cribl-leader.example.com:9000 Leader budget: 1,200 requests per hour, burst 150 Certificate verified	Enabled	Connected	12/10/2026, 13:48:30	

- 1

Cribl.Cloud or self-managed
An organisation and workspace with an API client, or a Leader URL with credentials and its TLS settings.
- 2

Connectivity result
Each connection is tested; the result and its time are shown.

- 3

Leader request budget
Every tenant on the connection shares it: TrackMe never overloads the Leader.
- 4

Read access only
The account reads configuration and Workers; TrackMe never writes to Cribl.

Connection & Worker Groups — the step that meets Cribl

Create a new TrackMe Virtual Tenant: Cribl Stream

1 Basics

2 Connection & Worker Groups

3 Indexes & RBAC

4 Review

Choose the Cribl connection: Its Worker Groups are listed from the Leader. Then choose the Splunk metric index its metrics arrive in.

Manage Cribl connections

Cribl connection

Cribl metric index

Metric prefix

Model learning history

cribl_cloud

Choose a metric index

cribl.logstream.

30 days

Where Splunk indexes this workspace's Cribl metrics.

Keep the default unless Cribl sends a custom prefix.

How far back the traffic ML models learn when the tenant is created.

Choose the metric index Cribl sends its metrics to

Cribl metrics (prefix cribl.logstream.) arrived in these indexes in the last hour. Use the one of this connection, or choose another in Cribl metric index above.

cribl_metrics

1 of 1 Worker of this connection report here

Use this index

cribl_metrics_docker

A Worker Group named default reports here, but none of this connection's Workers

Use this index

WORKER GROUPS

Waiting for the metric index

1 Worker Group found

Refresh discovery

Choose the metric index to see which Worker Groups send metrics there and select the ones to monitor.

default

Use one tenant per Cribl connection, with a metric index or a prefix of its own.

Choose the Cribl metric index.

Back

Next

1

Cribl connection

Its Worker Groups are listed from the Leader at once.

2

Cribl metric index

TrackMe finds the metric indexes where this connection's Workers report: Use this index.

3

Metric prefix

cribl.logstream. unless the deployment renames its metrics.

4

Model learning history

From today on, 7, 14, 30 (default), 60 or 90 days of history.

5

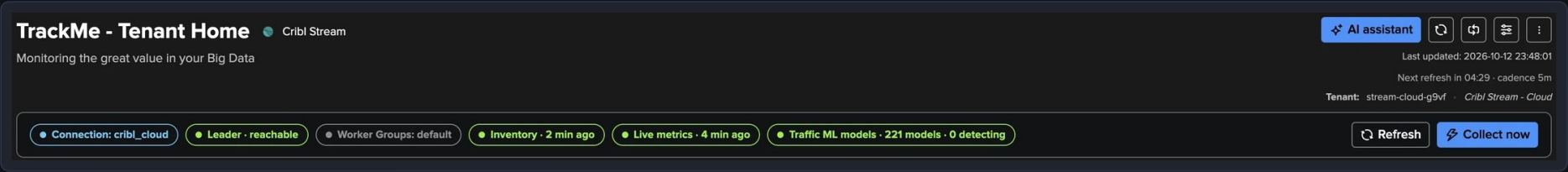
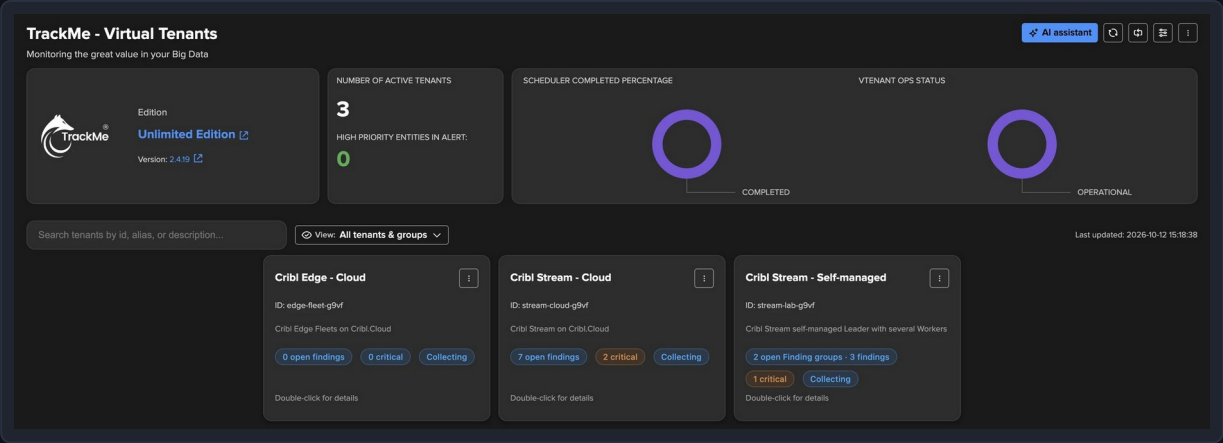
Worker Groups

All selected; keep the ones this tenant monitors (1 to 100).

TrackMe for Splunk • Hands-on: Cribl Stream

docs.trackme-solutions.com

The tenant card and the status strip



- 1

Tenant card
Open Finding groups and findings, critical ones, collection status.
- 2

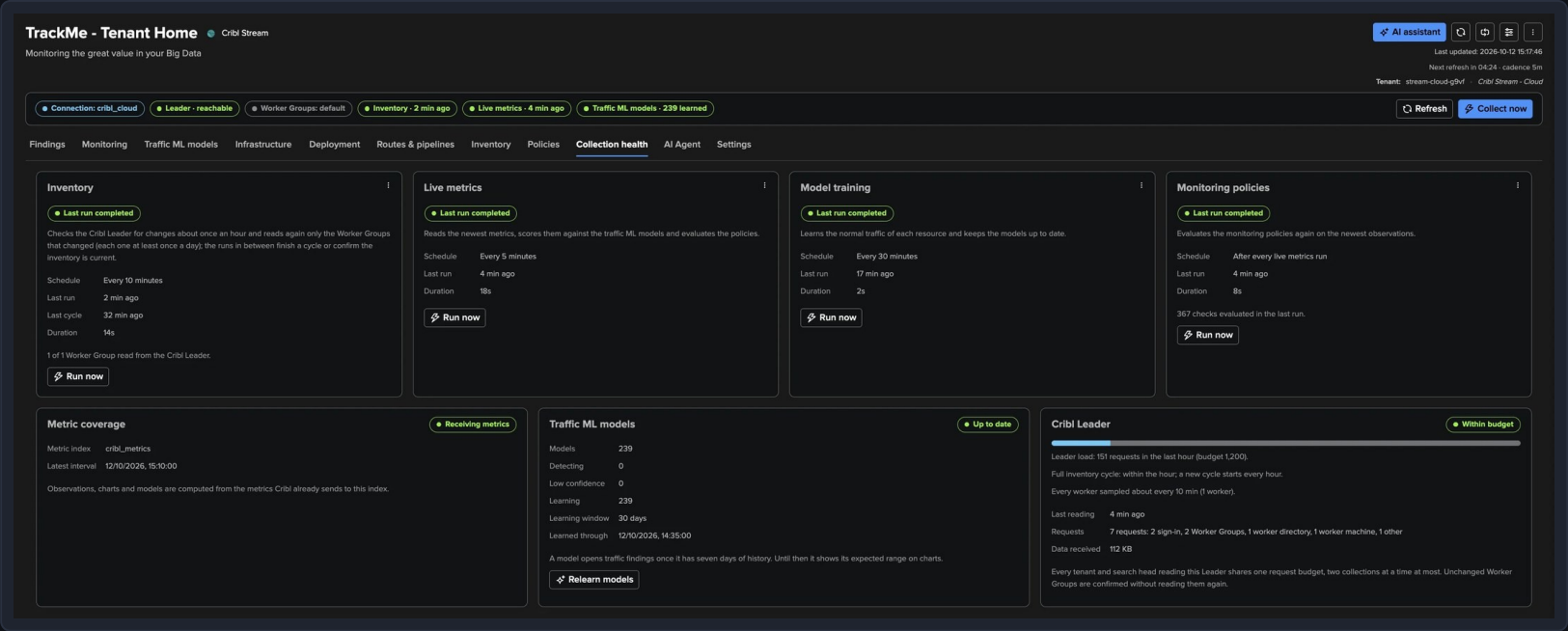
Connection and Leader
Reachable, unavailable, rate limited or unknown; hover for the reason.
- 3

Worker Groups
The Worker Groups the tenant monitors.
- 4

Jobs
Inventory, Live metrics and Traffic ML models with their last run.
- 5

Collect now
Reads the newest metrics and evaluates the policies at once.

Collection health — every job, its last run, its outcome in words



1 **One card per job**
Inventory, Live metrics, Model training, Monitoring policies, each with Run now.

2 **Metric coverage**
Receiving metrics, and any Worker Group that sends none.

3 **Traffic ML models**
Learning progress, learning window, Relearn models.

4 **Cribl Leader**
Requests of the last hour against the budget, the inventory cycle.

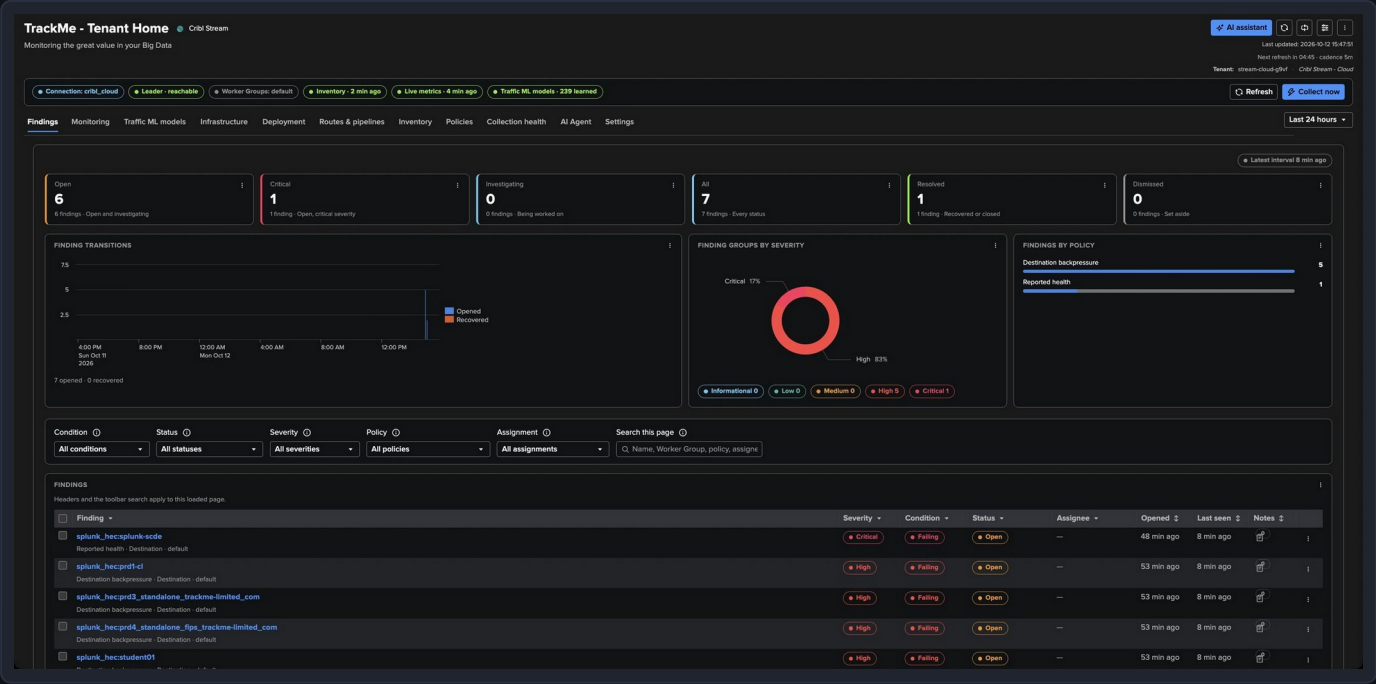
02

PART 2 • FINDINGS

Read, decide, route

The Findings tab, Finding groups and the triage, the investigation of a traffic outlier and of a Worker that went down, assignment rules and webhooks.

The Findings tab — the backlog, one row per Finding group



1 **Tiles**
Open, critical, investigating, all, resolved, dismissed.

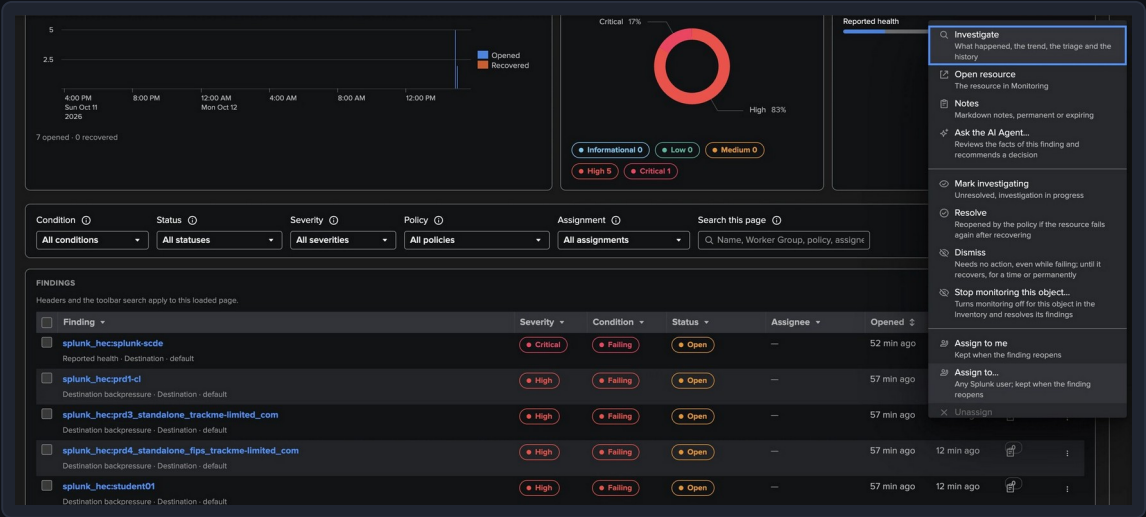
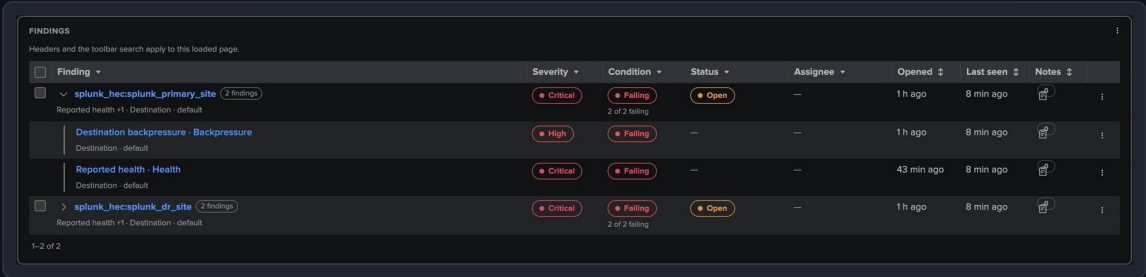
2 **Finding transitions**
Opened and recovered over the time range.

3 **By severity and by policy**
Destination backpressure and Reported health here.

4 **Filters and search**
Condition, status, severity, policy, assignment.

5 **Condition and status**
What the latest evaluation measures, and your decision.

Finding groups and the triage — one object, one decision

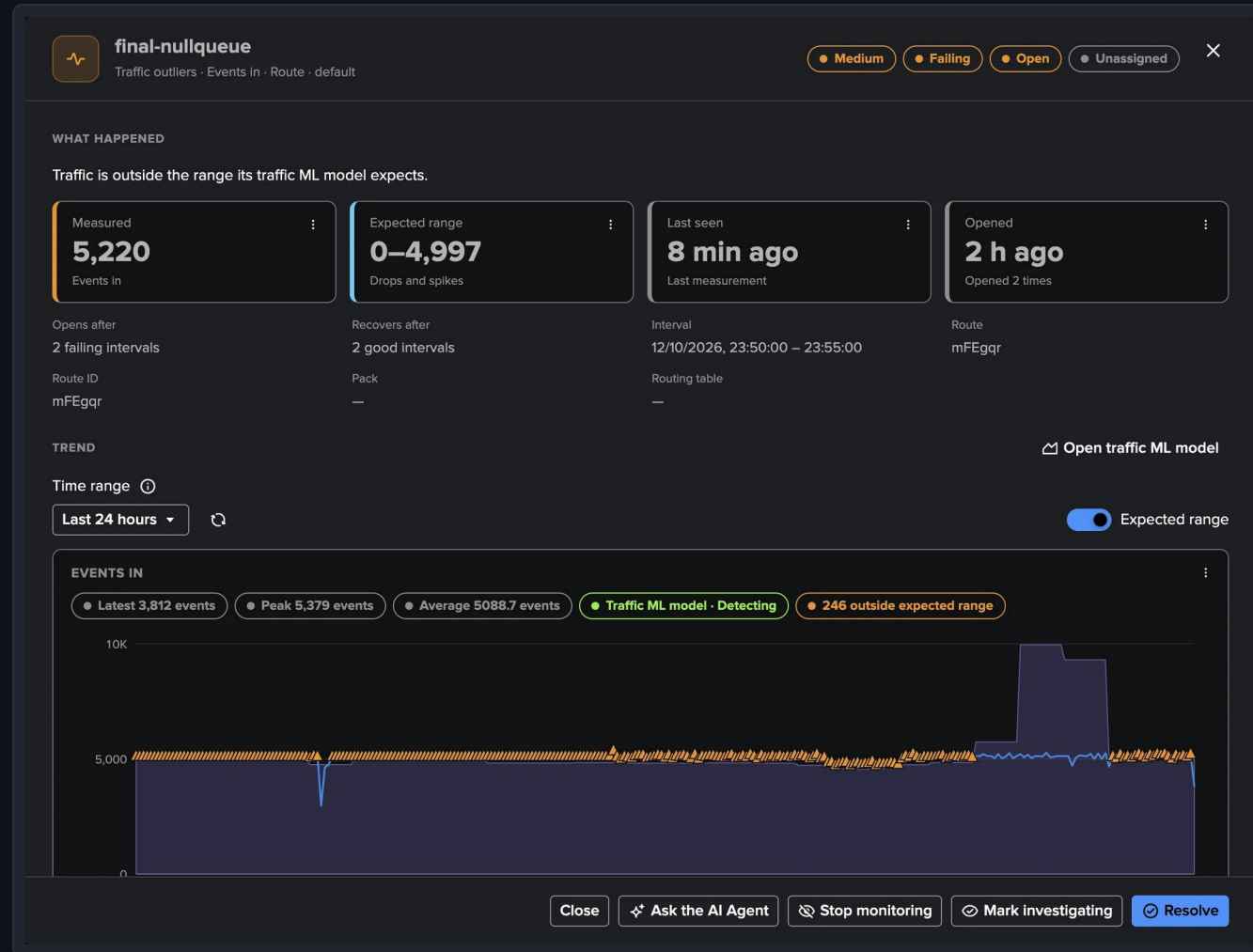


- 1 Automatic Finding groups**
A Worker whose CPU, memory and processes all run hot is one row.
- 2 Group severity**
The highest of its failing members; override possible.

- 3 Decisions**
Investigating, resolve, dismiss (until recovery, 1–90 days, permanently), reopen.
- 4 Assign, snooze, notes**
Snooze stops notifications without changing the status.

- 5 Stop monitoring this object**
Turns monitoring off and resolves its findings in one step.
- 6 Forget this object**
A removed or silent object, purged at once (administrator).

Investigating a traffic outlier — what happened, against what was expected



1 What happened

A Route measured 5,220 events against an expected 0–4,997.

2 Opens and recovers

After 2 failing intervals; recovers after 2 good ones.

3 The Route

Its id, Pack and routing table, from the Leader inventory.

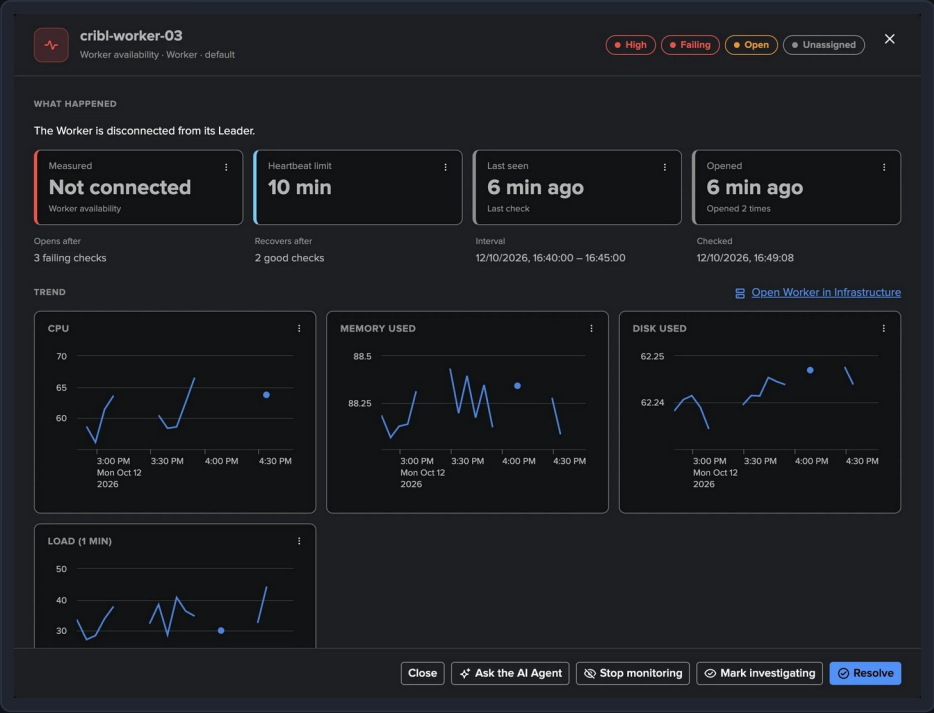
4 Trend with the expected range

The measurement over 24 hours with its band and the outlier points.

5 Decide here

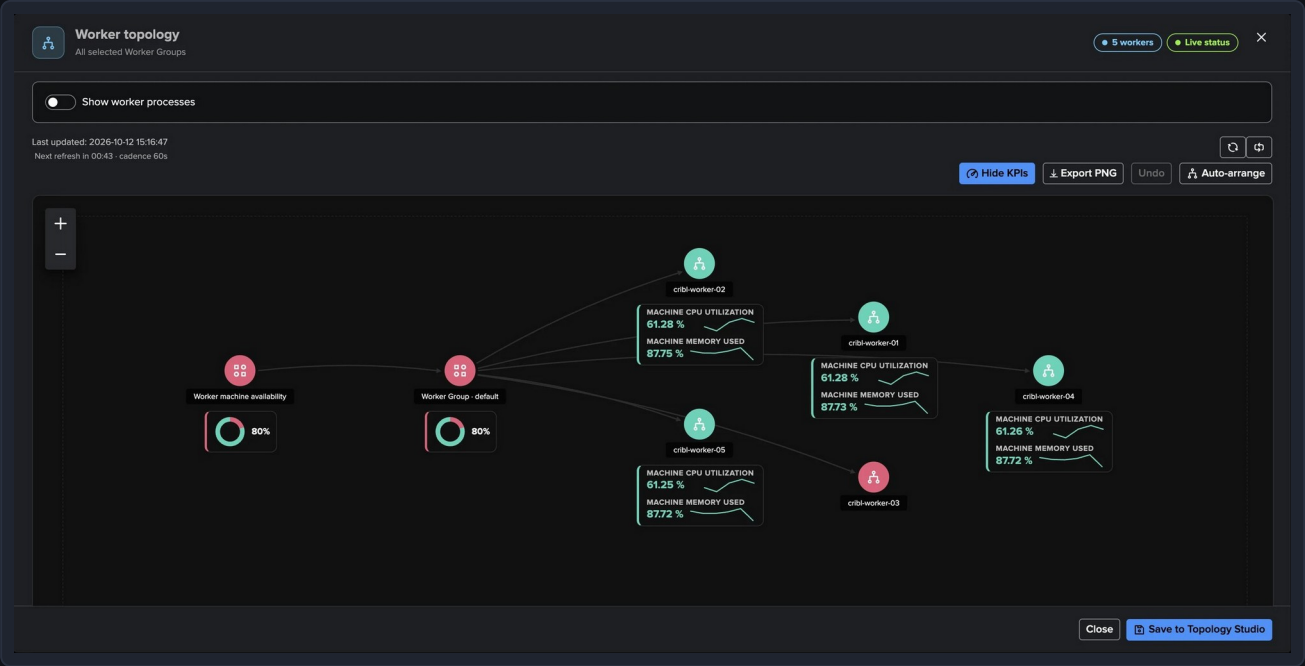
Ask the AI Agent, Stop monitoring, Mark investigating, Resolve.

A Worker goes down — the finding and the topology agree



1 **Worker availability**
High: disconnected, or no heartbeat for 10 minutes.

2 **The drawer**
The last heartbeat and the policy lines.



3 **Worker topology**
The crashed Worker red, the others green, processes shown.

4 **Drift and resources**
Version drift, configuration drift, machine CPU and disk, process CPU.

Assignment rules — the right team, automatically

AUTOMATIC ASSIGNMENT RULES

First matching rule wins. All criteria must match the same active finding; assignment applies to its whole Finding group. Empty criteria match every value. Manual decisions and existing assignees are preserved.

1. Destinations to the data platform team

Rule name

Destinations to the data platform team

☒ Enabled

Policy

Select...

Any selected value; empty means all.

Severity

Select...

Any selected value; empty means all.

Subject type

Destination X

Any selected value; empty means all.

Worker Group

Select...

Exact values or wildcard patterns (* and ?).

Object name / ID

Select...

Exact values or wildcard patterns (* and ?).

Destination type

Group

Assignment group

Data platform team

Move up

Remove rule

+ Add rule

GROUP NOTIFICATIONS

☐ Notify assigned groups automatically

Sends one message per Finding group and event using operator notification events, severity filters and delivery account. A group needs an email address. Account-owner notifications remain i

PREVIEW AND EXISTING FINDINGS

Preview matches

This page contains 6 Finding groups. Save rule changes before applying. Select up to 25 eligible groups.

☐ splunk_hec:prd4_standalone_fips_trackme-limited_com · default: Preserved: Group: Data platform team

☐ splunk_hec:prd1-ci · default: Preserved: Group: Data platform team

☐ splunk_hec:student01 · default: Preserved: Group: Data platform team

☐ splunk_hec:prd3_standalone_trackme-limited_com · default: Preserved: Group: Data platform team

☐ splunk_hec:student02 · default: Preserved: Group: Data platform team

☐ splunk_hec:splunk-scde · default: Preserved: Group: Data platform team

Apply to selected groups

1

Ordered rules

First match wins: policy, severity, subject type, Worker Group, object name.

2

An assignment group

Destinations go to the Data platform team.

3

Preview matches

The Finding groups a rule matches, before applying.

4

Manual decisions kept

Existing assignees are preserved; groups can be notified by email.

TrackMe for Splunk · Hands-on: Cribl Stream

docs.trackme-solutions.com

Findings actions — drilldowns, links and webhooks on every finding

Send webhook×
splunkhec:prd1-cl

Webhook action

Finding details (JSON webhook)

POST
application/json
{
 "webhook-id": "0233b9e65b5d4359bef237d28bde1f52"
}
{
 "component": "cribl_stream",
 "evidence": {
 "bucket_end": 1791816900,
 "bucket_start": 1791816600,
 "unit": "code",
 "value": 2
 },
 "finding": {
 "condition": "failing",
 "first_seen": 1791813300,
 "group_id": "857545f2f3c3fd43ee0ad13c146bd354a6d4fad83c9f4dbf1247710806f951ce",
 "id": "95d1745767a5967a0a1817601f8f1fc6e44d4bf1d736232e19c07a92f
tenant_id=stream-cloud-
g9vf&tab=evidence&health_view=findings&finding_id=95d1745767a5967a0a1817601f8f1fc6e44d4bf1d736232e19c07a92fbb1ea9e&group_id=857545f2f3c3fd43ee0ad13c146bd354a6d4fad83c9f4dbf1247710806f951ce
backpressure",
 "severity": "high",
 "status": "open",
 "title": "Destination backpressure: splunkhec:prd1-cl",
 "sent_at": 1791817381,
 "source": "trackme",
 "subject": {
 "entity_id": "splunkhec:prd1-cl",
 "entity_kind": "output",
 "event_host": "",
 "family": "outputs",
 "kpi": "backpressure_code",
 "label": "",
 "worker_group": "default",
 "tenant": {
 "alias": "stream-cloud-g9vf",
 "id": "stream-cloud-
g9vf"
 }
 }
 }
}

Close

Preview

Confirm and send

1

Webhook accounts

System-wide, HTTPS only, destination-restricted.

2

Per-policy actions

The policy editor's Actions tab offers them on its findings.

3

Automation rules

Run an action automatically, for example on a new critical finding.

4

Preview, then send

The rendered payload before it leaves; the last result kept.

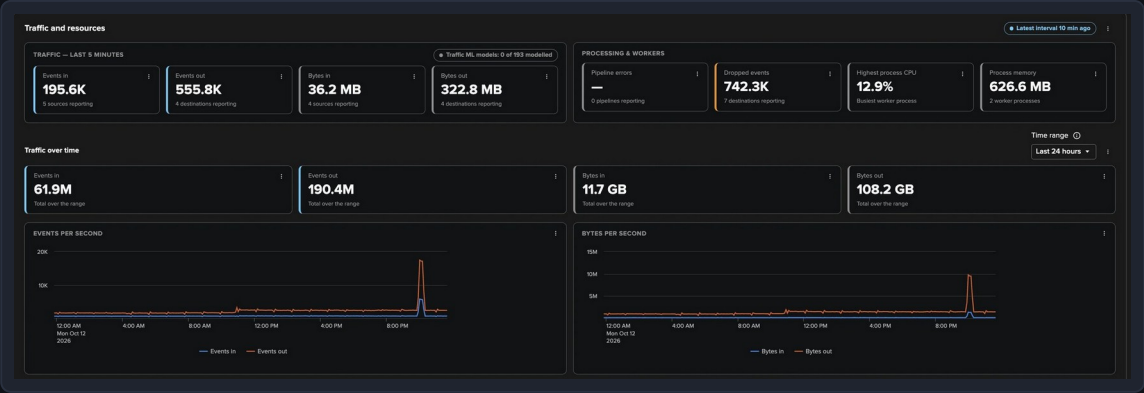
03

PART 3 · OBSERVE

Traffic, models, machines, data paths

Monitoring and its trends, the traffic ML models and their tuning, Expected traffic and silent objects, Workers and the Leader, Routes, Pipelines and the flow topology.

Monitoring — the newest interval and the last 24 hours



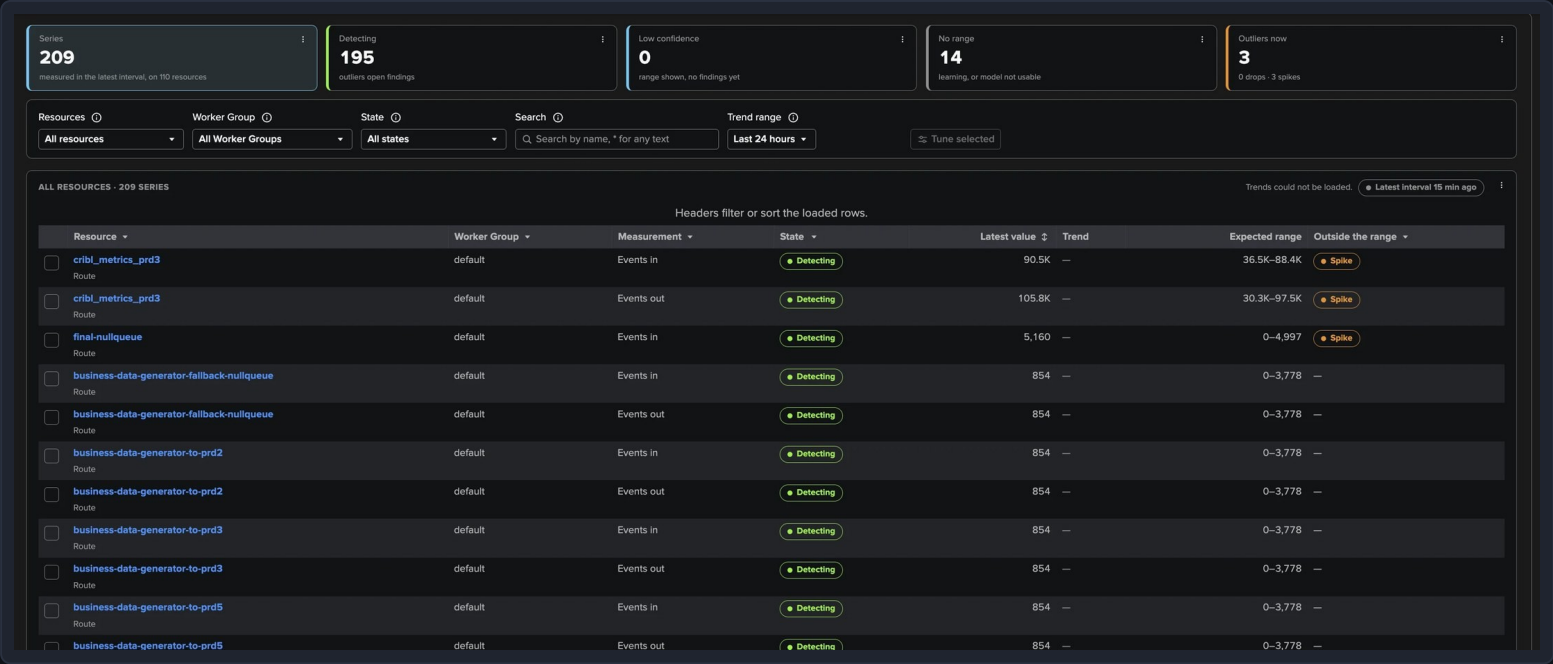
The 'Destinations' table lists various resources and their associated destinations. The table includes columns for Events out, Bytes out, Dropped, Trend, Health, and Model. The 'Health' column uses color-coded indicators: green for 'Healthy', red for 'Trouble', and grey for 'Learning'. The 'Model' column indicates the type of resource, such as 'Learning' or 'Trouble'.

Resource	Events out	Bytes out	Dropped	Trend	Health	Model
cribl_httpcribl_logstream	—	—	18.5K	—	—	—
elasticsearch	45.7K	16.8 MB	—	—	Healthy	Learning
google_chroniclesecops-akamai	—	—	—	—	Healthy	—
google_chroniclesecops-pan	—	—	—	—	Healthy	—
google_chroniclesecops-udm	—	—	—	—	Healthy	—
google_chroniclesecops-udm-akamai	—	—	—	—	Healthy	—
mail	—	—	234.4K	—	—	—
splunk_hacprst-cl	—	—	117.8K	—	Trouble	—
splunk_hacprst-current-release-fps	—	—	—	—	Healthy	—
splunk_hacprst-standalone_trackme-limited_com	176K	107.9 MB	—	—	Healthy	Learning
splunk_hacprst-standalone_trackme-limited_com	—	—	193.7K	—	Trouble	—
splunk_hacprst-standalone_fips_trackme-limited_com	—	—	9.444	—	Trouble	—
splunk_hacprst-s-cl	165.2K	98.5 MB	—	—	Healthy	Learning

- 1 Last five minutes**
Events and bytes in and out, dropped events, process CPU and memory.
- 2 Traffic over time**
Totals and per-second charts over the range.

- 3 Resource tables**
Each Destination with its traffic, drops, trend, health and model.
- 4 Reporting / No data**
The objects measured now, or those that stopped.

Traffic ML models — one per object and measurement



- 1

209 series, 195 detecting

14 without a range yet; 3 outside their range now.
- 2

Learning → Low confidence → Detecting

A range from one day, findings from seven days.
- 3

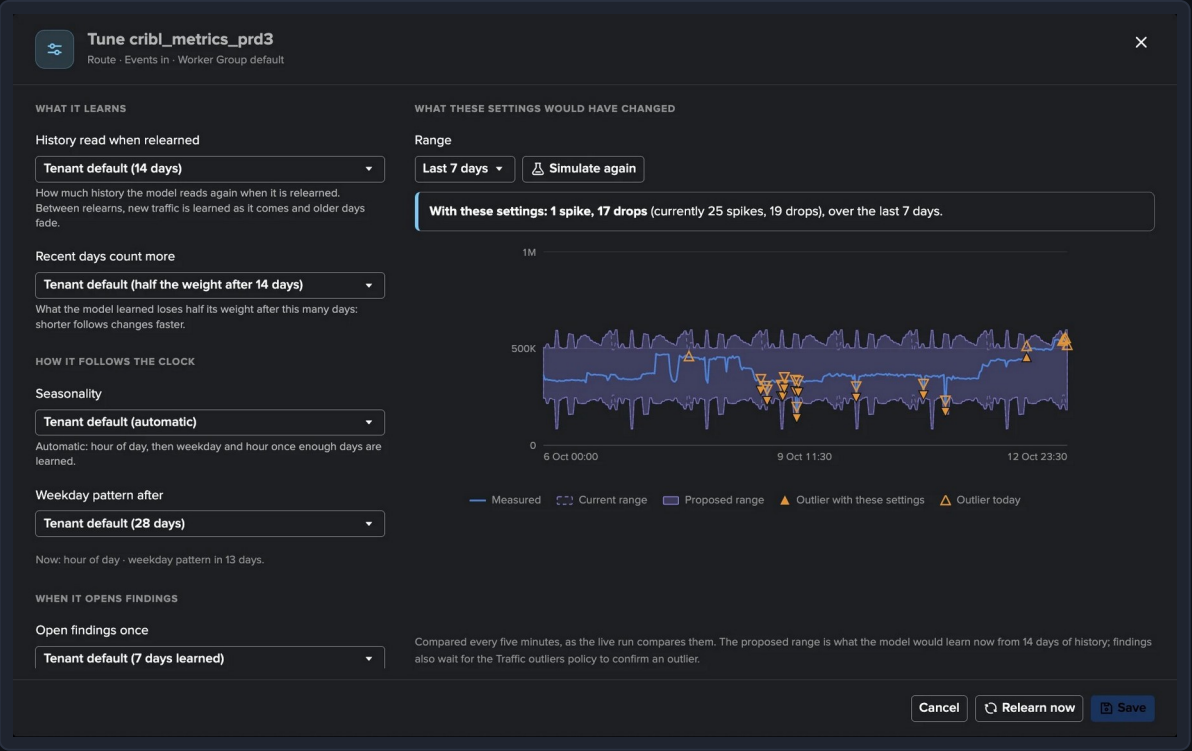
Expected range and Spike / Drop

The models outside their range come first.
- 4

Tune selected

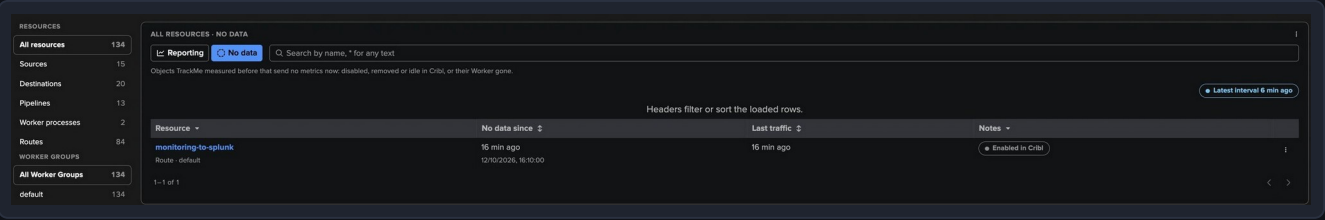
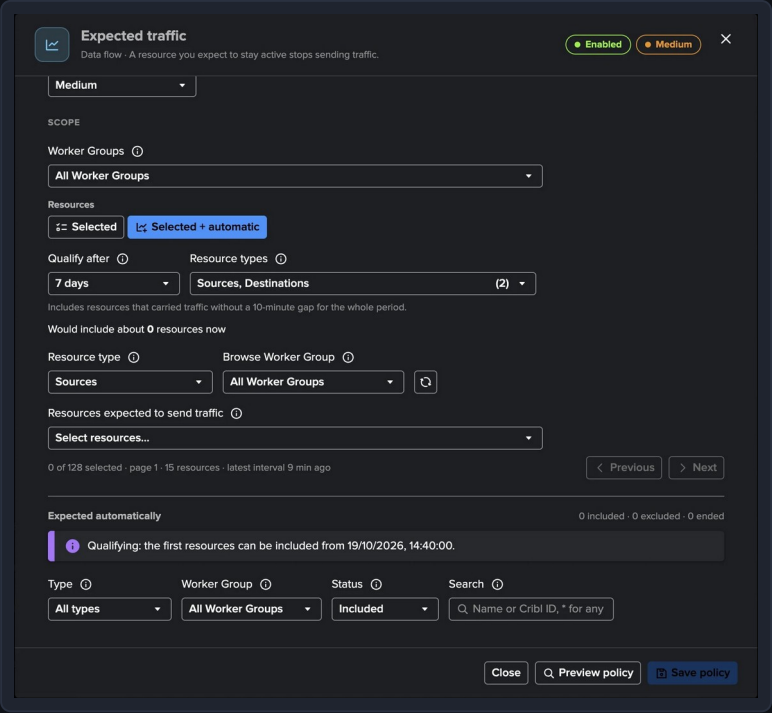
Give a selection of models its own settings.

A model, and what tuning it would change — before you save



- 1 14.9 days learned**
Hour-of-day seasonality; weekday pattern after 28 days.
- 2 Expected band and spikes**
24 spikes above the range in the last 24 hours.
- 3 Tune model**
History, recent days weight, seasonality, when findings open.
- 4 Live simulation**
Current and proposed ranges over 7 days: 1 spike and 17 drops instead of 25 and 19.
- 5 Not an anomaly**
An expected episode is excluded from learning and the finding dismissed.

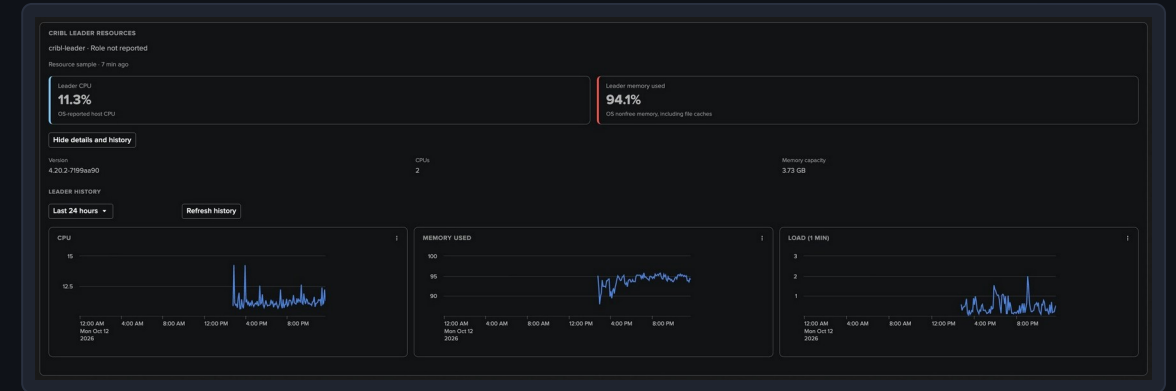
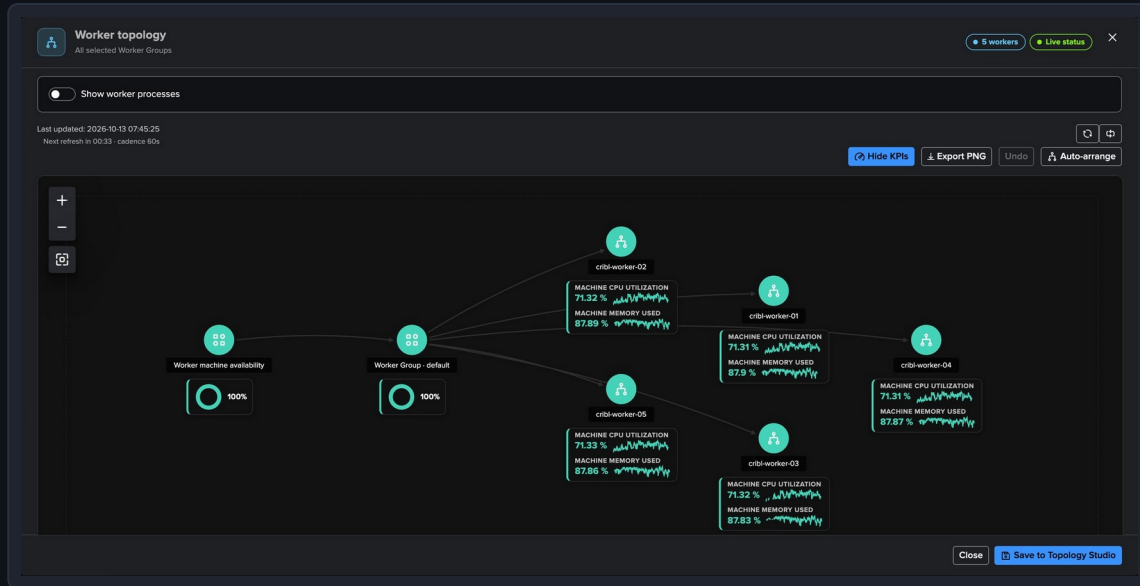
Expected traffic and objects that stop reporting



- 1 Expected traffic**
A finding when an object that must never go quiet carries no traffic.
- 2 Selected + automatic**
Every object with steady traffic over 7 days qualifies automatically.

- 3 No data**
Silent objects from their second missing interval, with their last traffic.
- 4 Silence counted carefully**
As zero traffic only when TrackMe is sure the silence is real.

Workers and the Leader — the machines behind Cribl Stream



1 Worker topology

The Worker Group and its Workers with CPU, memory and disk, live.

2 Save to Topology Studio

The map becomes a view that stays live.

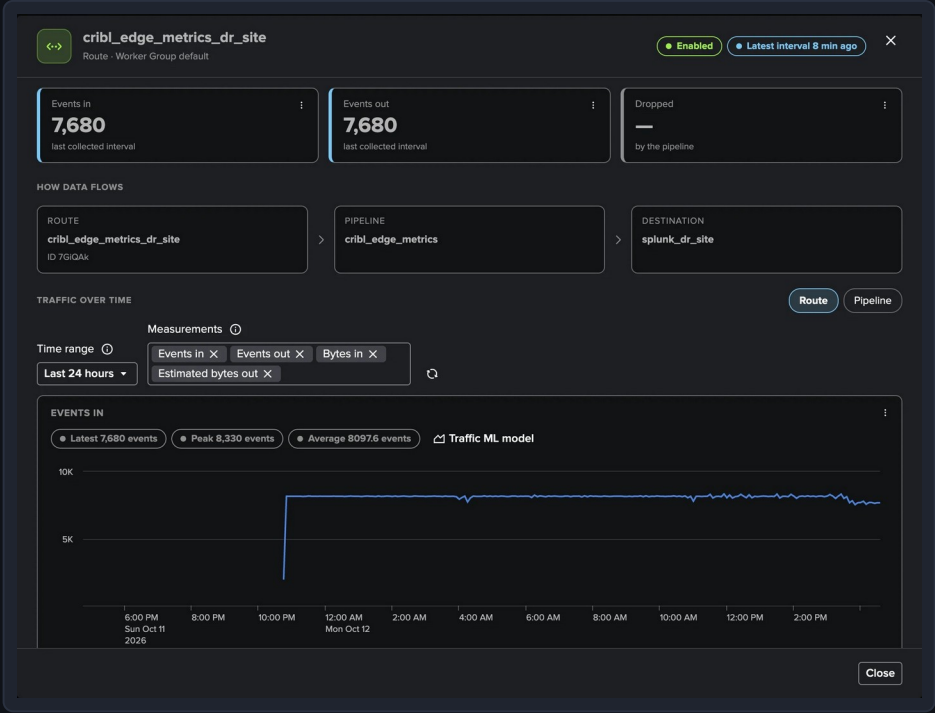
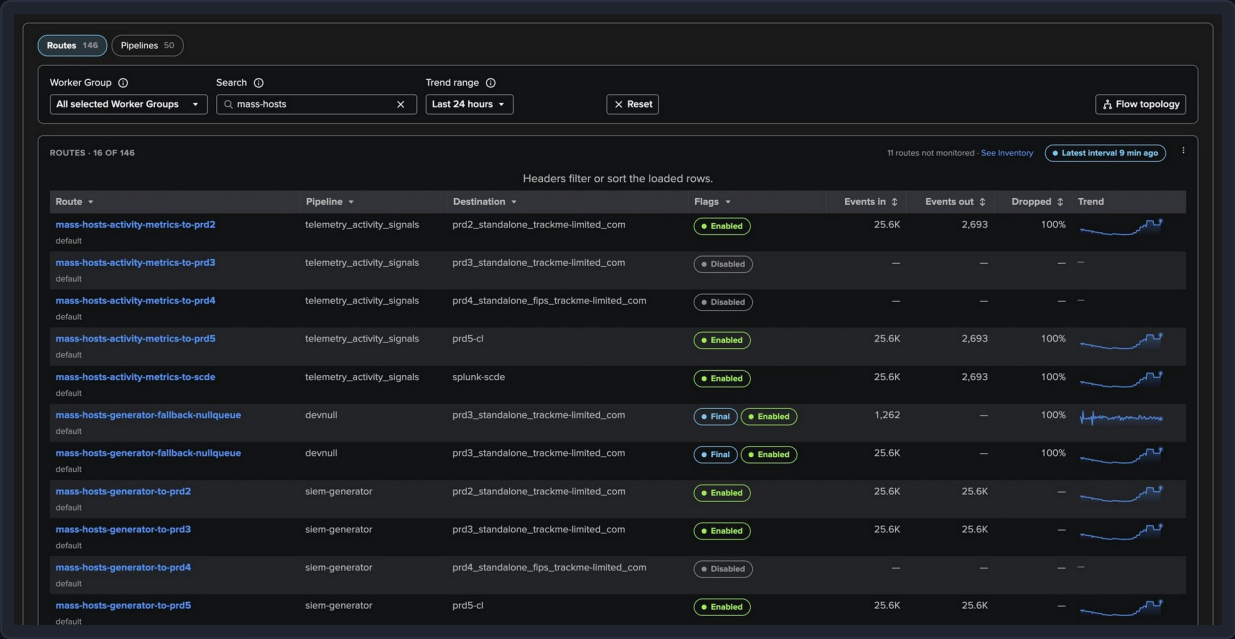
3 Leader resources

CPU, memory and load history of each Leader node.

4 Leader availability

A critical finding after two failed Leader API checks.

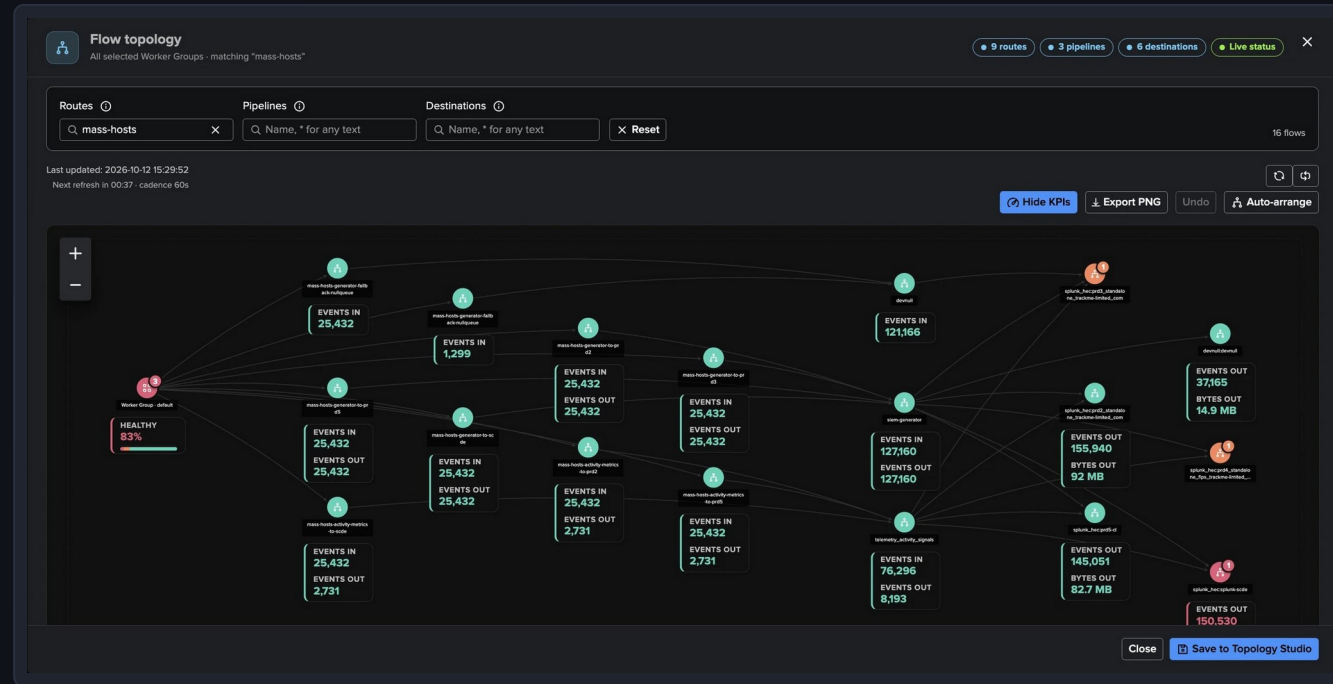
Routes & pipelines — how data flows, with its traffic



- 1 **Routes**
Each Route with its Pipeline and Destination, final or not, traffic and trend.
- 2 **Pipelines**
Functions, traffic, errors and drops.

- 3 **Search**
Filter by Worker Group or name; * stands for any text.
- 4 **Configured processing path**
A Route opens its traffic with Route → Pipeline → Destination beside it.

Flow topology — your data paths, drawn for you



- 1 Worker Group → Route → Pipeline → Destination**
Read from the Leader, joined with the traffic.
 - 2 Live KPIs and findings**
Events, bytes and health on every node; Live status every minute.
 - 3 Nothing invented**
A link only when both ends are measured.
 - 4 Export or save**
Export PNG, or Save to Topology Studio as a live view.

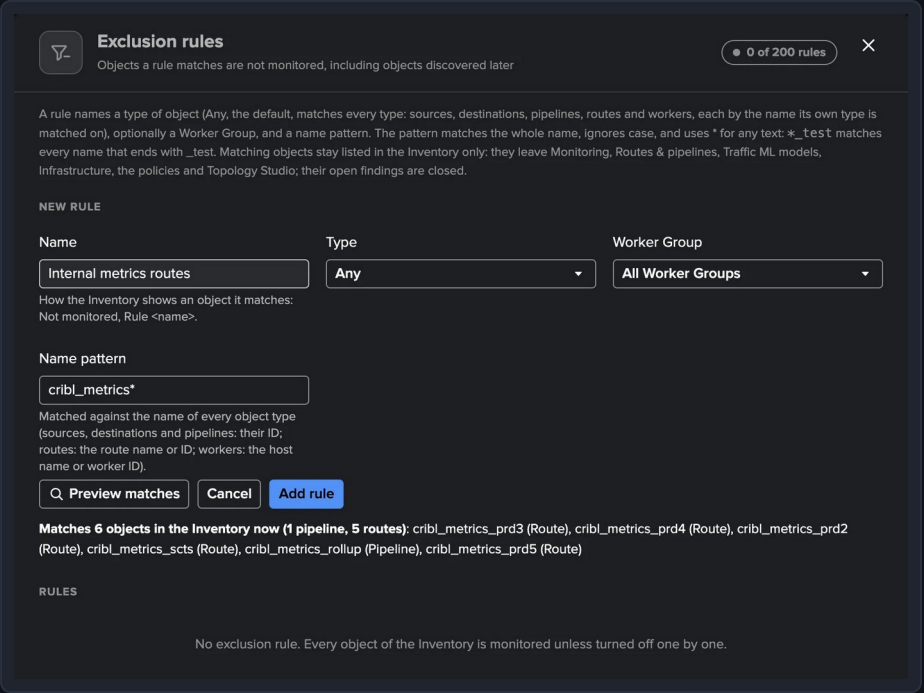
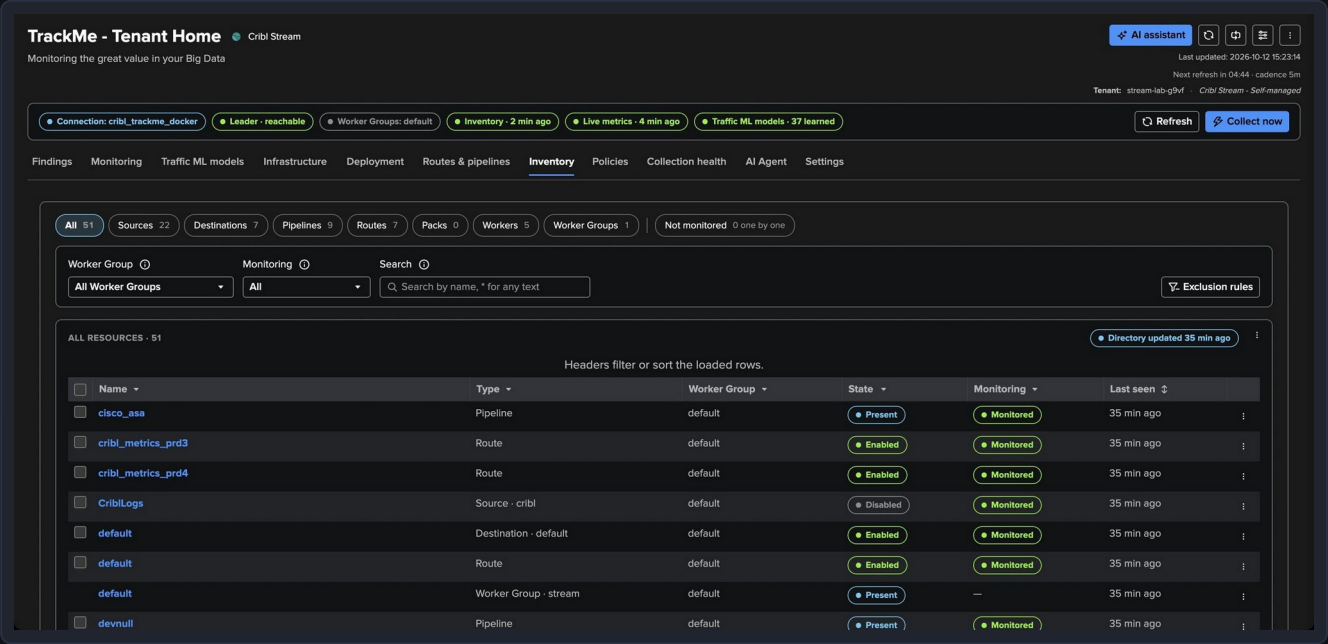
04

PART 4 • OPERATE

Scope, rules, people, AI

Inventory and exclusion rules, the policy catalogue, notifications, the Cribl Stream AI Agent, Topology Studio, the AI Assistant and the Configuration Guardian.

Inventory and exclusion rules — monitor what matters



1 Every object the Leader reports
Per type and Worker Group, with first and last seen.

2 Monitoring on or off
One by one, or with exclusion rules by type, Worker Group and name.

3 Preview matches
What a rule excludes, before saving.

4 Out of every tab
An excluded object leaves the policies, models and Topology Studio.

Sixteen policies in four groups — 14 on out of the box

POLICIES • 14 OF 16 ENABLED

A policy opens a finding when its condition holds and closes it once it recovers.

All 16

Cribl Leader 4

Data flow 5

Worker processes 1

Worker machines 5

View List

Policy	Category	Status	Severity	Conditions	Scope	Actions
Leader availability TrackMe cannot reach or use the configured Leader API.	Cribl Leader	Enabled	Critical	Opens after 2 checks - recovers after 2	Configured Leader API	Edit
Leader CPU An observed Leader node runs high on CPU.	Cribl Leader	Enabled	Medium	Opens after 3 checks - recovers after 2 - threshold 90%	Each observed Leader node	Edit
Leader memory An observed Leader node runs high on memory.	Cribl Leader	Disabled	Medium	Opens after 3 checks - recovers after 2 - threshold 90%	Each observed Leader node	Edit
Leader disk A Leader filesystem runs high on disk usage.	Cribl Leader	Enabled	Medium	Opens after 3 checks - recovers after 2 - threshold 90%	Each observed Leader filesystem	Edit
Reported health A source or destination reports an unhealthy state in Cribl.	Data flow	Enabled	Medium - Critical on trouble	Opens after 3 intervals - recovers after 2	All Worker Groups - all resources	Edit
Traffic outliers Traffic drops or spikes compared with what its traffic ML model expects.	Data flow	Enabled	Medium	Opens after 2 intervals - recovers after 2 - drops and spikes 0 Detecting 0 Low confidence 221 Learning	All Worker Groups - all resources	Edit
Expected traffic A resource you expect to stay active stops sending traffic.	Data flow	Enabled	Medium	Opens after 3 intervals - recovers after 1	Selected + automatic - 0 selected - 0 automatic	Edit
Pipeline errors A pipeline reports processing errors.	Data flow	Enabled	Medium	Opens after 3 intervals - recovers after 2 - 1 error or more	All Worker Groups - all resources	Edit
Destination backpressure A destination reports backpressure or is blocked.	Data flow	Enabled	High - Critical when blocked	Opens after 2 intervals - recovers after 2	All Worker Groups - all resources	Edit
Process CPU A worker process stays busy on CPU.	Worker processes	Enabled	Medium	Opens after 3 intervals - recovers after 2 - threshold 90%	All Worker Groups - all resources	Edit
Worker machine CPU A worker machine runs high on CPU.	Worker machines	Enabled	Medium	Opens after 3 checks - recovers after 2 - threshold 90%	All Worker Groups - all workers	Edit
Worker machine memory A worker machine runs high on memory.	Worker machines	Disabled	Medium	Opens after 3 checks - recovers after 2 - threshold 90%	All Worker Groups - all workers	Edit
Worker machine disk The filesystem reported by a worker runs high on disk usage.	Worker machines	Enabled	Medium	Opens after 3 checks - recovers after 2 - threshold 90%	All Worker Groups - all workers	Edit
Worker availability A worker disconnects or stops sending heartbeats.	Worker machines	Enabled	High	Opens after 3 checks - recovers after 2 - heartbeat within 10 min	All Worker Groups - all workers	Edit
Worker version drift	Worker machines			Opens after 3 checks - recovers after 2	All Worker Groups - all workers	Edit

- 1

Cribl Leader
Availability, CPU, memory, disk.
- 2

Data flow
Reported health, Traffic outliers, Expected traffic, Pipeline errors, backpressure.
- 3

Workers
Process CPU, machine CPU, memory and disk, availability, version and configuration drift.
- 4

Open and recover
Consecutive checks to open and to recover, thresholds and scope.
- 5

Editor tabs
General, Actions and Automations.

Notifications — every transition indexed, emails when you want them

Notifications

Email the transitions of this tenant's findings. Every transition is also written as an event to the index `trackme_notable` (sourcetype `trackme:cribl::finding`), whatever these settings.

Enable notifications

☒ Email the transitions of findings

One email per live run listing the transitions of the run (digest), or one email per transition threaded per finding.
Delivery runs after the live metrics run, every 5 minutes, so a triage decision is notified within 5 minutes; collection never waits for it.

Events

☒ Finding opened

A policy confirmed a new failure.

☒ Finding reopened

It failed again after a recovery, or someone reopened it.

☒ Finding added to the group

Another finding of the same object joined its open Finding group.

☒ Severity raised

The severity rose (policy or manual).

☐ Severity changed

The severity was lowered or given back to the policy.

☒ Measurement recovered

The measurement recovered; an open finding is resolved.

☐ Resolved

Someone resolved it.

☐ Dismissed

Someone dismissed it.

☐ Marked not an anomaly

A traffic outlier marked not an anomaly.

☒ Dismissal ended

A dismissal for a time ended: the finding is open again.

☐ Marked investigating

Someone is investigating.

☒ Closed automatically

Nothing will measure it again (source changed, object not monitored, model paused...).

☐ Episode ended

A finding already closed lost its episode.

☐ Assigned

Someone was assigned.

☐ Unassigned

The assignee was removed.

☐ Snoozed

Snoozed for a while.

☐ Snooze cleared

The snooze was cleared.

☐ Findings of the group changed

Findings were grouped, removed from a Finding group or ungrouped by hand.

Transitions that are notified.

Minimum severity

Medium and above

Findings below this severity are not notified.

Policies

Every policy

Leave empty to notify for every policy.

Delivery account

corporate_smtp

An email delivery account from Configuration; the default sends through the local MTA of the search head.

Recipients

cribl-ops@example.com X

Up to 50 addresses, filtered by the allowed email domains of the delivery account.

Mode

☒ Digest — one email per live run

☐ Per finding group — one threaded email per transition of a Finding group

A digest lists every transition of a run; per finding threads the emails of one finding together.

Include charts

☒ Embed charts in the emails

Each email shows the finding chart and the key measurements of each object over the last 24 hours (up to 10 objects per digest).

Last delivery: Notifications are off.

Send test email

- 1

Indexed events

Every transition in the notable index, for Splunk alerts, ES or SOAR.
- 2

Events and severity

Opened, reopened, escalated, recovered...; Medium and above by default.
- 3

Digest or per Finding group

One digest per run, or one threaded email per group.
- 4

Charts inline

The objects' charts in the email; Send test email.

The Cribl Stream AI Agent — facts first, then a recommendation

Ask the AI Agent

Cribl Stream AI Agent

Inspect first

Finding: splunk_hecs:splunk-scde

Critical

SUMMARY

The finding is a critical reported health failure on the destination splunk_hecs:splunk-scde in the default Worker Group. The destination is present and referenced by many routes, with recent healthy traffic activity and no evidence of being disabled or inactive. The finding is currently failing and critical, with no recovery observed. The evidence indicates a real problem requiring operator attention rather than a false positive or expected behaviour.

FINDINGS ASSESSED (1)

True Positive

splunk_hecs:splunk-scde

Reported health

High confidence

Decision: Mark Investigating

Evidence: The destination 'splunk-scde' is present, not disabled, referenced by 18 routes, and carries significant recent traffic. The finding condition is failing with critical severity and no measured recovery. Traffic models are in learning phase, so no anomaly dismissal applies. The finding history and system records confirm a critical reported health failure.

The finding represents a critical health failure on a destination actively used and carrying traffic, with no evidence of false positive or inactivity. Resolving or dismissing is not allowed by preconditions. The best decision is to keep the finding under investigation to allow operators to assess and resolve the real issue.

Reasoning trace

1 [AI Agent] note written or updated in the finding notes.

Close

Run its recommendations...

1

Checked facts

First seen, disabled in Cribl, gone from the Inventory, Routes, traffic, model.

2

An assessment

True positive, likely false positive, not in use, expected, needs investigation.

AI Agent

Scheduled triage off

Mode: Inspect

Provider: first available

Not scheduled

AI enabled

Provider configured

Owner can run agents

Settings

Run a review now

Scheduled triage is off. The agent can still be asked about a finding, or to review the open findings now.

Time range

Kind

Mode

Outcome

Decision

Launched

Last 7 days

Everything

All modes

All outcomes

All decisions

Scheduled or asked

Scheduled runs

Findings reviewed

Recommendations

Actions taken

Refused

Inspect / Act

0

1

1

0

0

1 • 0

Runs of the scheduled triage

1 review

Reviews recommending a change

Decisions applied as AI Agent

Decisions TrackMe refused

1 asked • 0 scheduled

DECISIONS

Headers filter or sort the loaded rows.

Time	Mode	Finding	Decision	Outcome	Rationale
34 min ago	Inspect	splunk_hecs:splunk-scde	Review - True positive	Recorded	The finding represents a critical health failure on a destination actively used and carrying traffic, with no evidence of false positive or inactivity. Resolving or...
	Asked	Reported health - default	Recommends: Mark Investigating		

3

Inspect or act

Act applies only what the tenant allows; never a permanent dismissal.

4

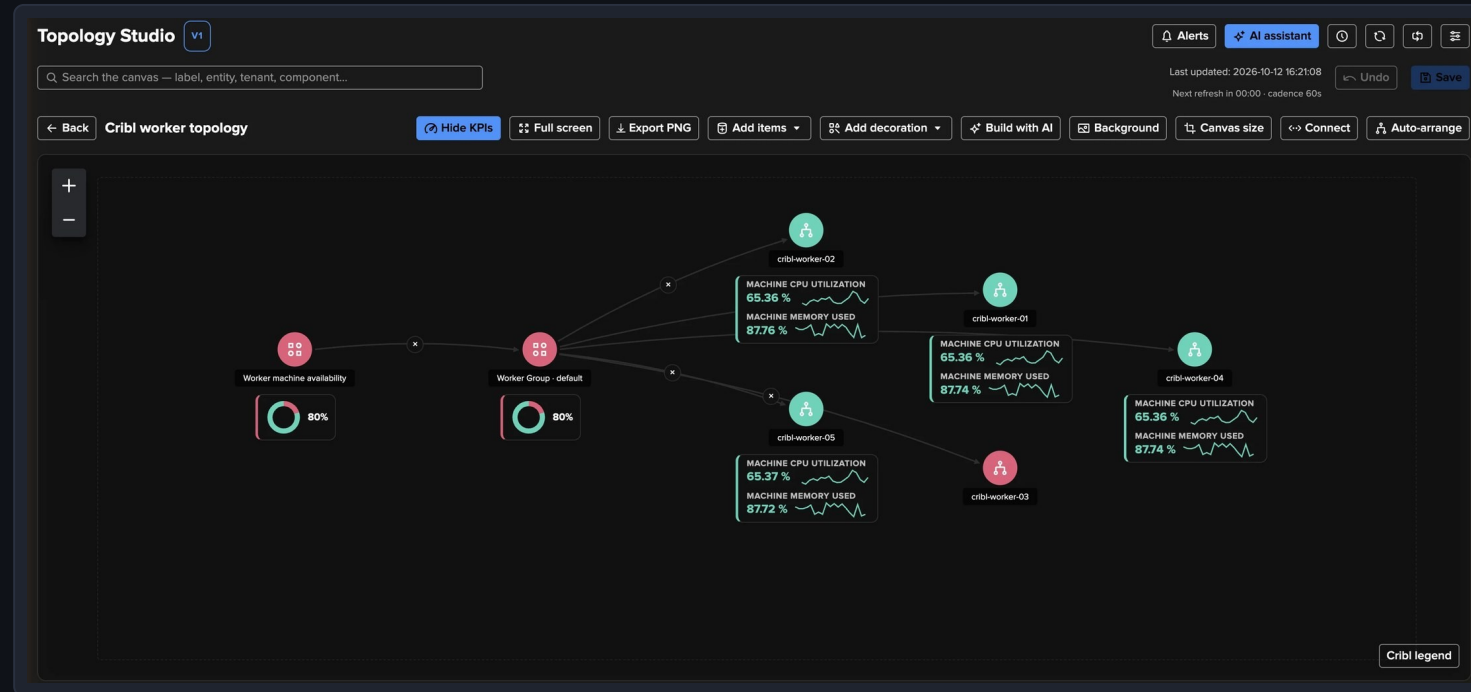
Decision log

Every review, asked or scheduled; hourly triage off by default.

TrackMe for Splunk • Hands-on: Cribl Stream

docs.trackme-solutions.com

Cribl objects in Topology Studio — live, coloured by their findings



1

From the workspace

Flow, Worker and Process topologies saved as live views.

2

Dynamic Cribl groups and templates

Five templates, from Flow of a Worker Group to Problems wall.

3

Live state

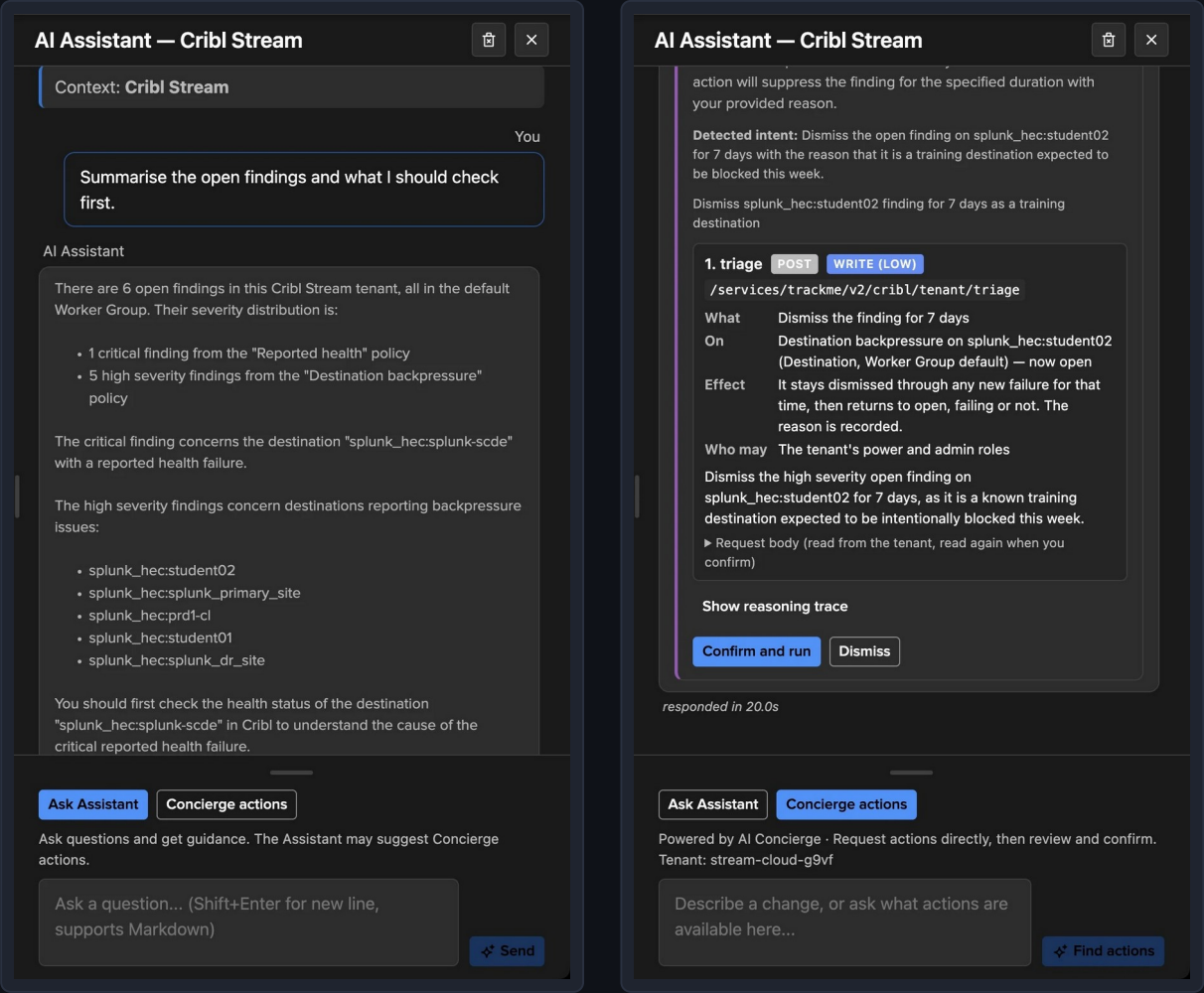
Red, orange, blue when snoozed, green, grey when not measured.

4

Alerts and AI

Topology Alerts and Build with AI know Cribl objects.

The AI Assistant and the Concierge — ask, then confirm



- 1

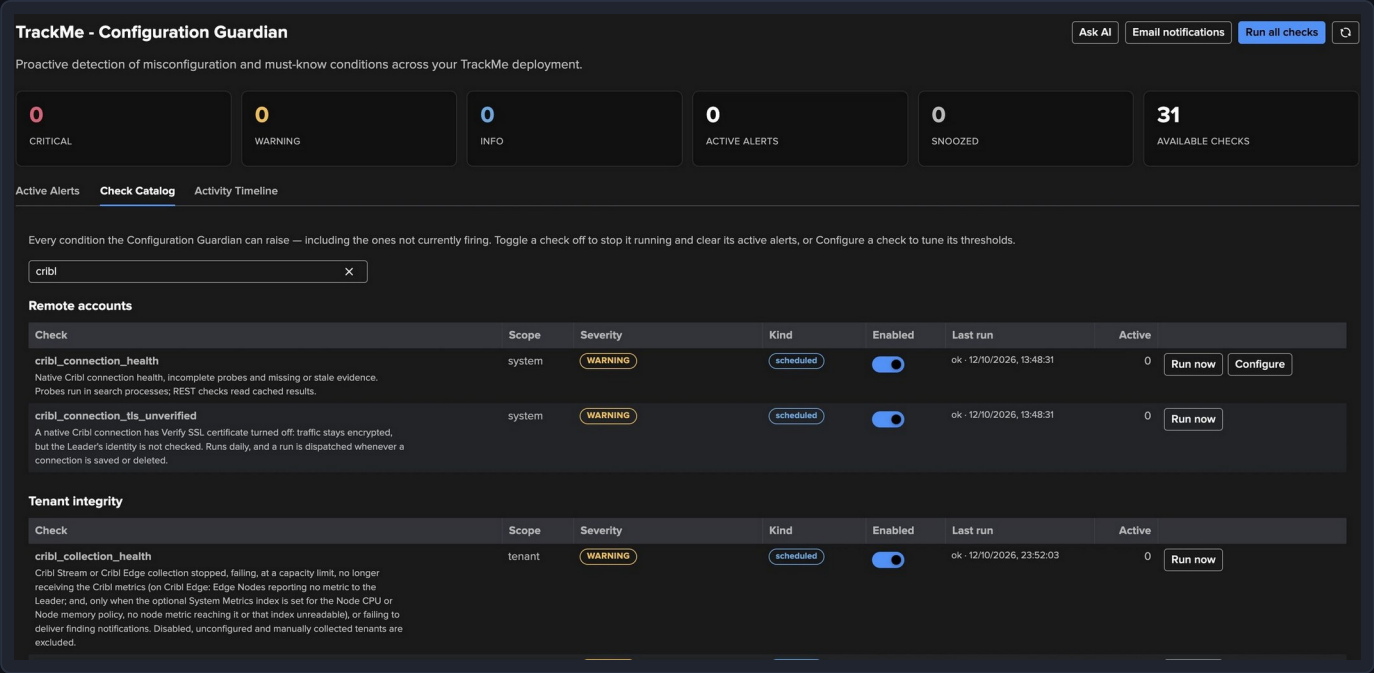
Grounded in the tenant
Findings, traffic ML models, collection health, monitoring state, Leader load.
- 2

Ask why
Why a finding is open, what to check in Cribl, when a model is ready.
- 3

Concierge consent card
What, On, Effect, Who may — confirmed before it runs.
- 4

Roles kept
Policies, exclusion rules, tuning and settings stay in the workspace.

The Configuration Guardian — never trust a silent tenant



- 1

cribl_collection_health
A job not running or failing, metrics not arriving, a Worker Group sending none.
- 2

Load and scale
The inventory cycle or worker sampling slowing under the Leader budget.

- 3

Connections
cribl_connection_health and cribl_connection_tls_unverified.
- 4

Each problem with its next step
And it clears itself when the condition ends.

Where we are

In four parts

● Set up

a Cribl connection, the wizard and the first collection, checked in Collection health

● Triaged

Finding groups decided once, an outlier and a Worker failure investigated, findings routed

● Observed

traffic, traffic ML models and their tuning, Workers, the Leader and the data paths

● Operated

inventory, policies, notifications, the AI Agent, Topology Studio and the Guardian

What made it work

Read what you already have

Cribl's own metrics, in place, and the Leader API within its budget. Nothing installed, nothing changed in Cribl.

Normal, learned per object

A traffic ML model per object and hour, explained, tunable with a simulation before saving.

One decision per object

Finding groups, assignment, webhooks and an AI Agent that checks facts before recommending.