



HANDS-ON WALKTHROUGH · CRIBL EDGE

Is every Edge Node where it should be?

One tenant follows the Fleets of a Cribl Edge Leader, the Edge Nodes enrolled in them and the Sources and Destinations they run — connected nodes, rollouts that reached every node, versions, failing inputs and outputs, full disks — at any fleet size.

Captured live on TrackMe 2.4.19 · a Cribl.Cloud Edge Fleet of 17 nodes



An Edge fleet fails one node at a time — silently

A handful of servers or tens of thousands of endpoints: nobody can open each node to check it.

Nodes that drop

A collector shut down, a fifth of a Fleet disconnected after a network change — and the data of those hosts stops.

Rollouts left behind

A deploy that did not reach every node, nodes left on an old Edge version after an upgrade.

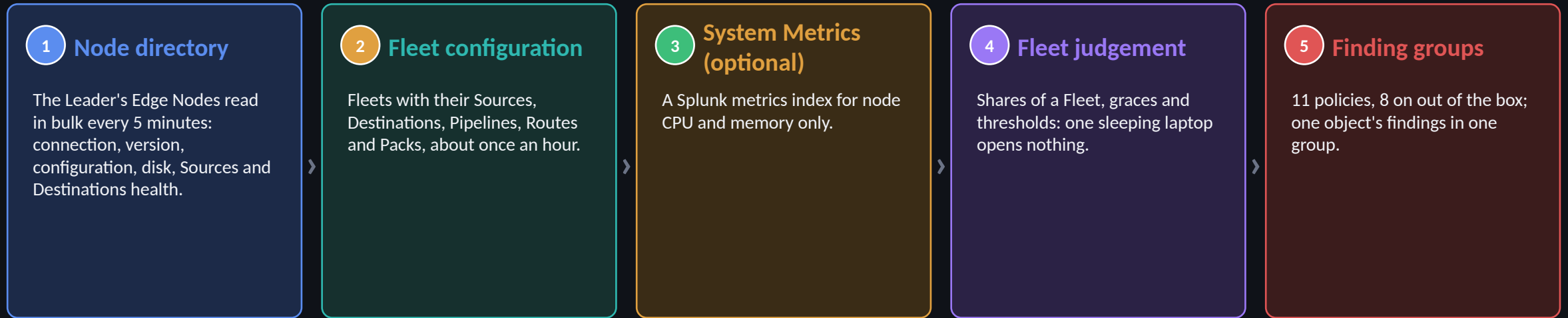
Inputs and outputs failing

A Destination in trouble on 4 of 17 nodes, a disk filling up on one host.

What a Cribl Edge tenant does

A dedicated tenant type on a Cribl connection to the Edge Leader. TrackMe reads the Leader's node directory in bulk at every run — no call per node, no node limit — judges each Fleet as a share of its nodes, and raises findings from eleven built-in policies. Nothing is installed or changed on Cribl.

One bulk read of the Leader, judged per Fleet, at any size



Detail on demand

A node's CPU, memory, network and disk activity, and the live status of one of its Sources or Destinations, are read from the Leader only when someone opens that node: the fleet-wide collection stays one bulk read.

No traffic ML models for Edge: endpoints are sparse and irregular, and there can be very many of them. Explicit, explainable rules instead.

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

PART 1

Setup

- The Cribl Edge card
- Connection & Fleets
- The workspace and its strip

PART 2

Fleets & nodes

- The Fleets tab
- A Fleet, and its nodes to look at
- Edge Nodes, one node up close

PART 3

Findings

- The Findings tab
- A disconnected node, nodes that must stay connected
- Version drift

PART 4

Operate

- Policies, bank holidays, collection health
- Settings, Topology Studio, the assistant
- The AI Agent and its instructions

Every screen is the product as shipped, on a Cribl.Cloud Edge Fleet.

01

PART 1 • SETUP

One connection, one Leader, one tenant

The Cribl Edge card, the Connection & Fleets step with its optional System Metrics index, and the workspace with its status strip.

A dedicated tenant — pick Cribl Edge

Create a TrackMe Virtual Tenant

Splunk Feeds Tracking

Monitor and track Splunk data feeds

- SPLK-DSM: data source monitoring
- SPLK-DHM: event endpoint tracking
- SPLK-MHM: metric endpoint tracking

SPLK-DSM

Select

Splunk Volume (Outliers)

Licensed volume drops and spikes per index

- Outliers on the licensed volume of every index
- Daily licensed volume and month projection
- Local or remote, history backfilled on day 1

Select

Splunk Fields Quality Monitoring

Assess and monitor data quality at scale

- Create sampling jobs for CIM and non-CIM
- Generate quality dictionaries
- Detect and alert on quality issues

Select

Splunk Workload

Track and manage scheduled report activities

- Discover and monitor schedules
- Detect anomalies and trends
- Optimize workload costs

Select

Splunk Flex Objects Tracking

Track entities from your “magic searches”

- Register searches producing objects
- Status and KPIs via simple conventions
- Workflow & metrics ingestion automated

Select

User Activity Monitoring

Investigate Splunk user activity and policy findings

- Local or remote environment
- Human and service account classification
- Evidence, collection gaps and investigation workflow

Select

Cribl Stream

Monitor the health and traffic of your Cribl Stream workspace

- Sources, destinations, pipelines, routes and workers
- Findings from health, traffic outliers and worker policies
- Computed from your Cribl metrics, no extra ingestion

Select

Cribl Edge

Monitor your Cribl Edge Fleets and Edge Nodes at any scale

- Node connectivity per Fleet, version and configuration drift
- Source and Destination health reported by the nodes, disk hotspots
- From the Cribl Leader API, no extra ingestion

Select

Close

1 The Cribl Edge card

Node connectivity per Fleet, version and configuration drift, Source and Destination health, disk hotspots.

2 From the Leader API

No extra ingestion: the Leader is the source.

3 Four steps

Basics, Connection & Fleets, Indexes & RBAC, Review.

Licence

A valid Enterprise, Unlimited, trial or Developer licence. Not available on the Foundation edition or the Foundation trial.

Virtual Tenants → Actions → Create a tracking tenant.

Connection & Fleets, then review

Create a new TrackMe Virtual Tenant: Cribl Edge

1 Basics

2 Connection & Fleets

3 Indexes & RBAC

4 Review

Choose the Cribl connection: its Edge Fleets are listed from the Leader. The Leader API is the source; a System Metrics index is only needed to monitor node CPU and memory.

[Manage Cribl connections](#)

Cribl connection

cribl_cloud

System Metrics index (optional)

cribl_metrics_edge

Only needed to monitor the CPU and memory of your Edge Nodes with the Node CPU and Node memory policies: the Splunk metrics index receiving the Edge System Metrics source of your Fleets (node-* metrics). TrackMe uses it for nothing else. Without it, everything else works the same. Node disk included: the Leader API is the source.

FLEETS

Listed

1 of 1 Fleet selected

Refresh listing

default_fleet

17 Edge Nodes

Use one tenant per Cribl connection. A Subfleet can be monitored with its parent or on its own.

Back

Next

- 1

Cribl connection

Locked once the tenant exists: another Leader takes another tenant.
- 2

Fleets listed from the Leader

All selected on a first listing, with their node count; 1 to 100 Fleets.

Create a new TrackMe Virtual Tenant: Cribl Edge

1 Basics

2 Connection & Fleets

3 Indexes & RBAC

4 Review

REVIEW

Tenant	Connection	Fleets	System Metrics Index
edge-docs (Cribl Edge - Cloud)	cribl_cloud	default_fleet	cribl_metrics_edge
Scheduled collection	Owner	Roles	
On	svc-trackme	admin: trackme_admin · power: trackme_power · user: trackme_user	

Update comment (optional)

Back

Done

- 3

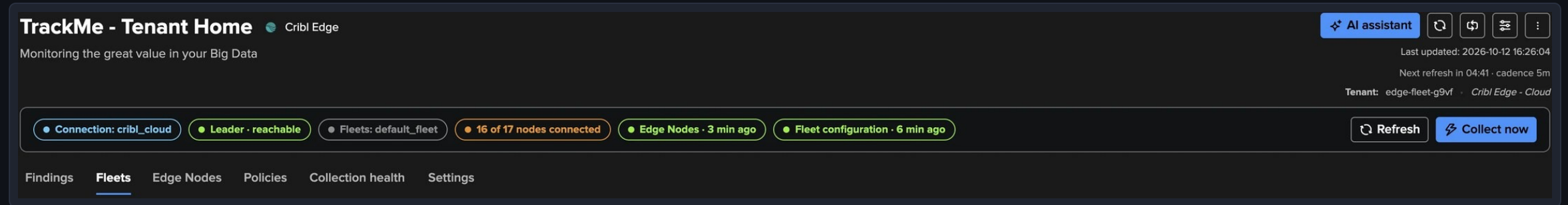
System Metrics index (optional)

Only for Node CPU and Node memory.
- 4

Review and create

The first collection starts at once; nodes appear within minutes.

The workspace — six tabs and a strip that sums it up



1

Connection and Leader

Reachable, with the time of the last check.

2

N of M nodes connected

From the latest node directory.

3

Edge Nodes and Fleet configuration

The age of the last run of each job.

4

Collect now

Reads the Edge Nodes and evaluates the policies at once.

5

Six tabs

Findings, Fleets, Edge Nodes, Policies, Collection health, Settings.

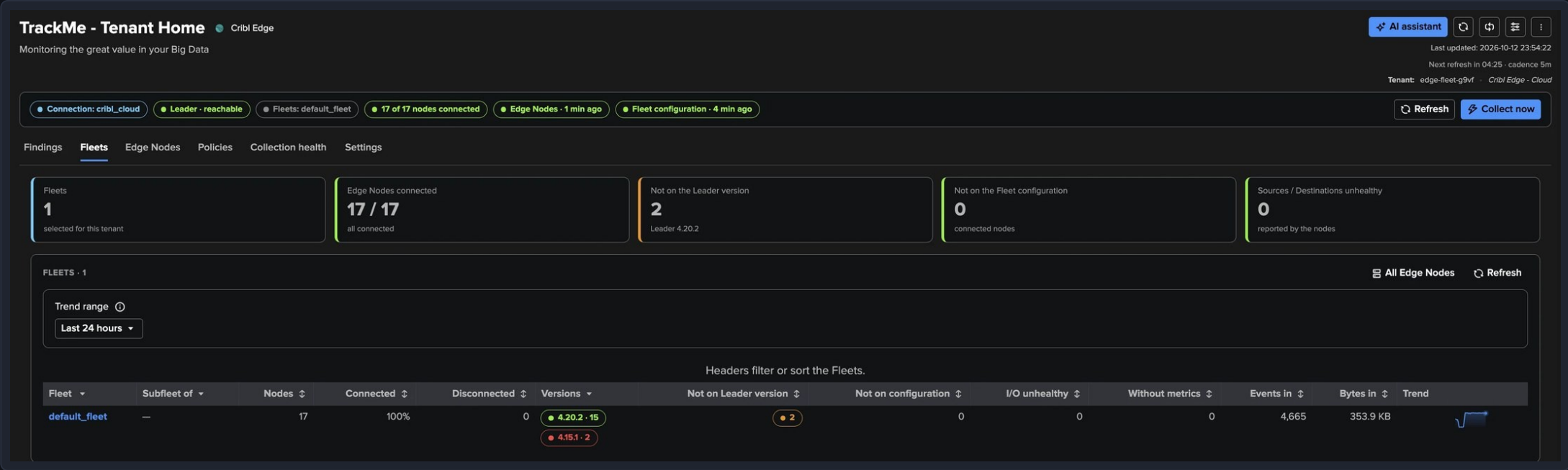
02

PART 2 • FLEETS & NODES

The fleet at a glance, any node up close

The Fleets tab and a Fleet with its nodes to look at; the Edge Nodes tab; one node with its info, its System activity read live and its data activity.

The Fleets tab — the fleet questions, answered at a glance



- 1 **Edge Nodes connected**

17 / 17 here; one click lists the disconnected ones.
- 2 **Not on the Leader version**

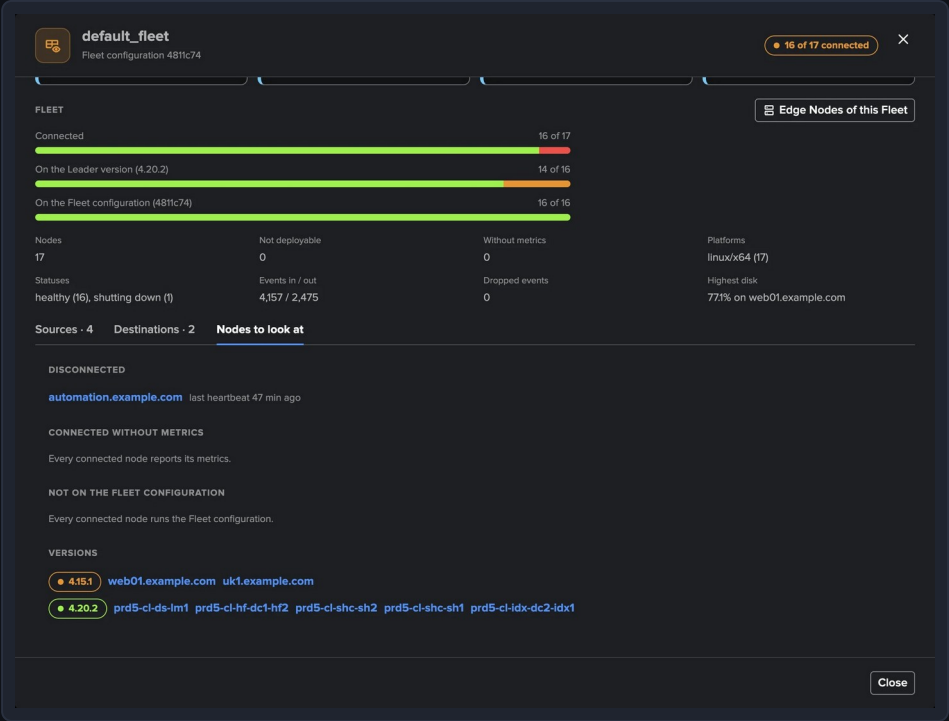
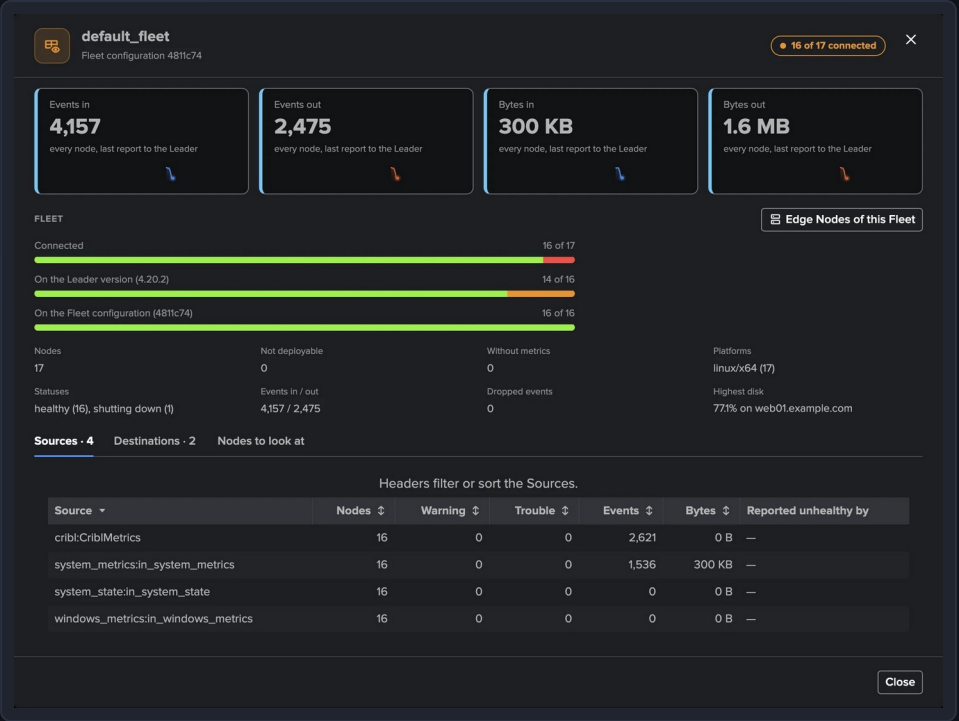
2 nodes behind Leader 4.20.2.
- 3 **Not on the Fleet configuration**

Connected nodes not running the deployed configuration.
- 4 **Sources / Destinations unhealthy**

Reported by the nodes themselves.
- 5 **One row per Fleet**

Nodes, connected share, versions, drift, traffic and trend.

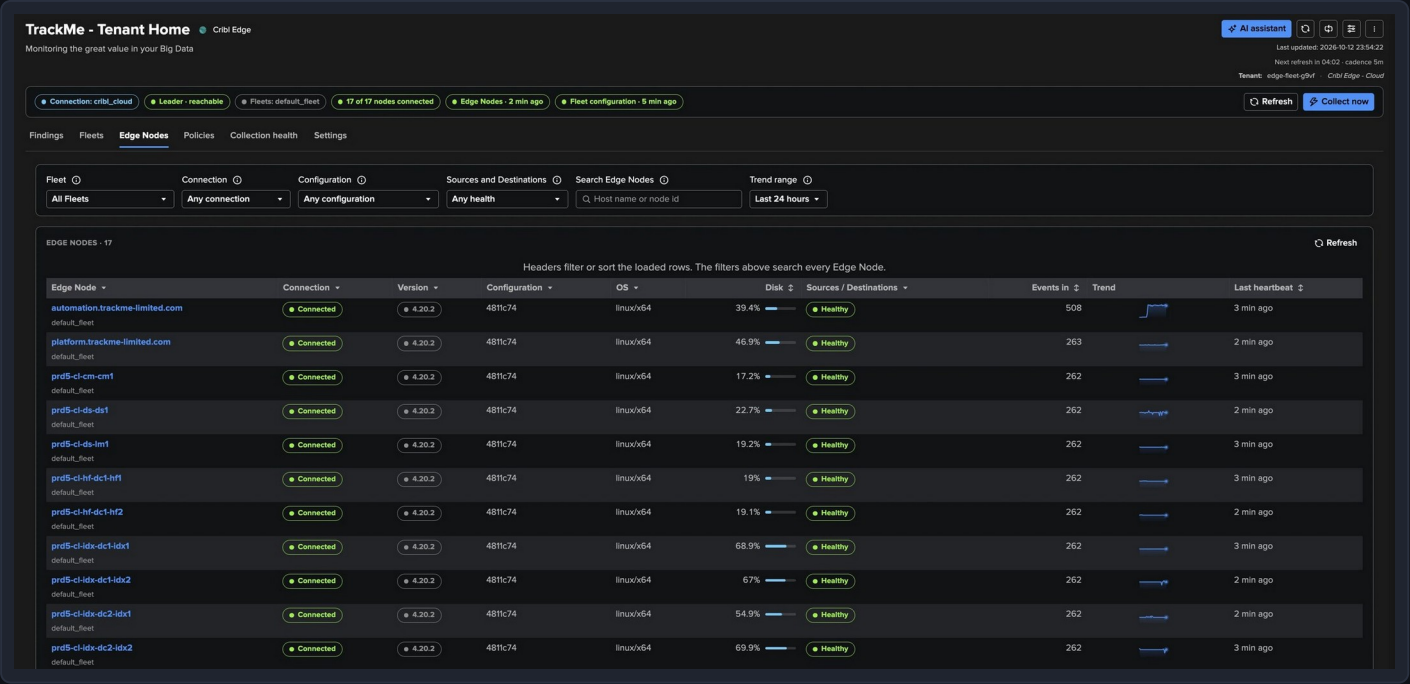
A Fleet — its traffic, its bars, and the nodes to look at



- 1 Traffic tiles with trends**
Events and bytes in and out: how busy the Fleet is now.
- 2 Three bars**
Connected, on the Leader version, on the Fleet configuration.

- 3 Sources and Destinations**
Nodes reporting each one, warning and trouble counts.
- 4 Nodes to look at**
Disconnected nodes, nodes off the configuration, the nodes behind each version.

Edge Nodes — paged and filtered by the server, at any size



1 Filters

Fleet, connection, configuration, Sources and Destinations health.

2 Search every node

Host name or node id, across the whole fleet.

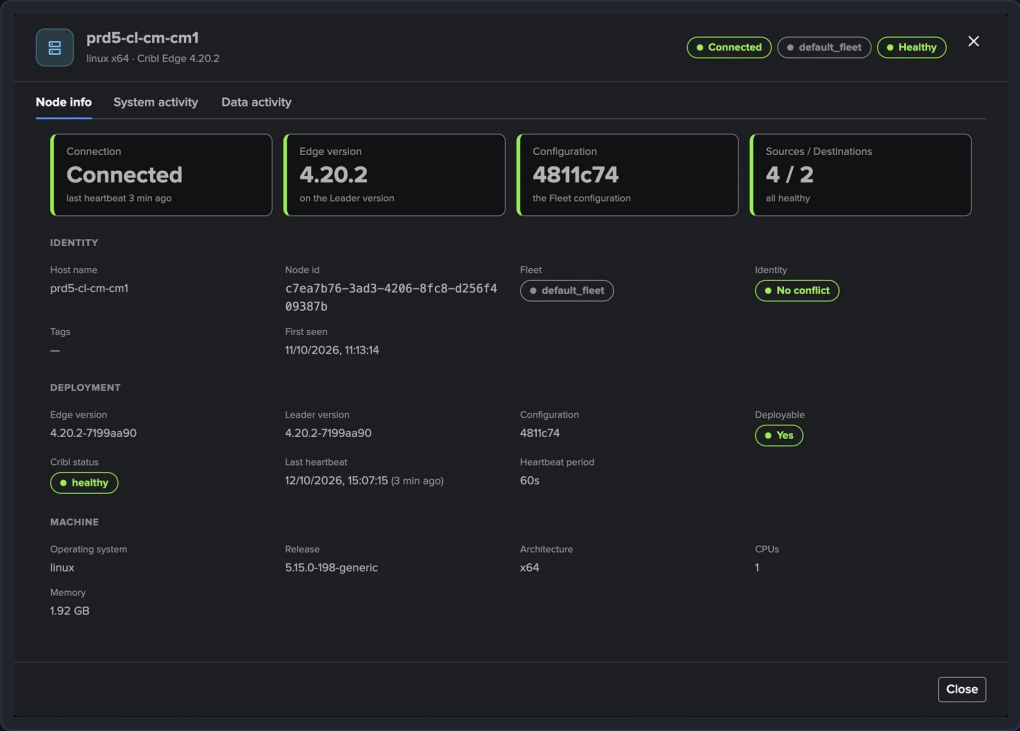
3 Per node

Connection, version, configuration, OS, disk, health, events in, trend.

4 No metrics never reads healthy

A connected node without metrics is shown as such.

One node — identity, deployment, machine, and its data



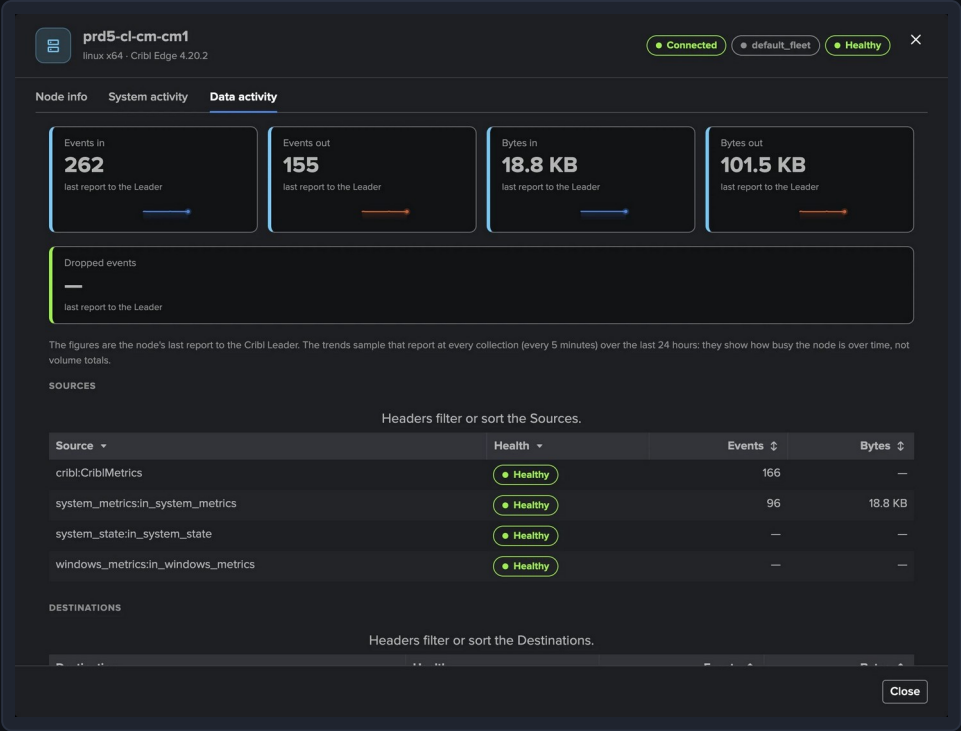
- 1

Four tiles

Connection, Edge version against the Leader, configuration, Sources / Destinations.
- 2

Identity and deployment

Host name, node id, cloned-image check, versions, heartbeat.



- 3

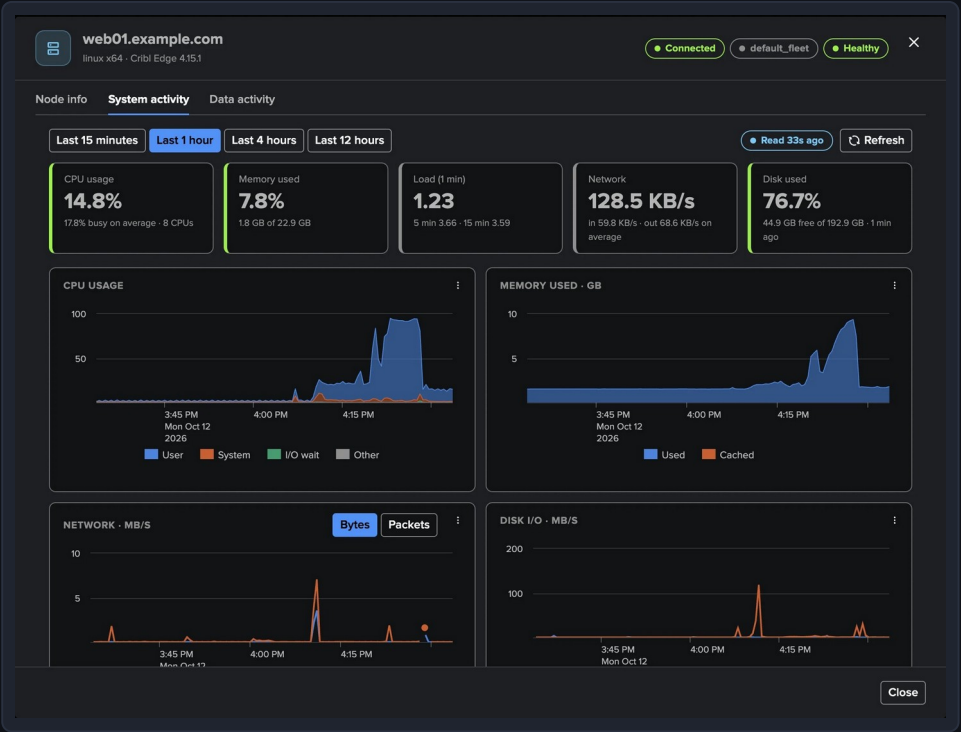
Data activity

Traffic tiles with 24-hour trends, from the node's last report to the Leader.
- 4

Sources and Destinations

Their health; select one for its live status from the Leader.

System activity — read live from the node, nothing to forward



- 1 What Cribl's System Activity shows**
CPU by mode, memory, network, disk I/O, load, processes.
- 2 15 minutes to 12 hours**
From the node's own store, through the Leader.

- 3 Only when opened**
Nothing read for a node nobody opens; within the Leader budget.
- 4 Disk history**
Kept by TrackMe for every node from its heartbeats.

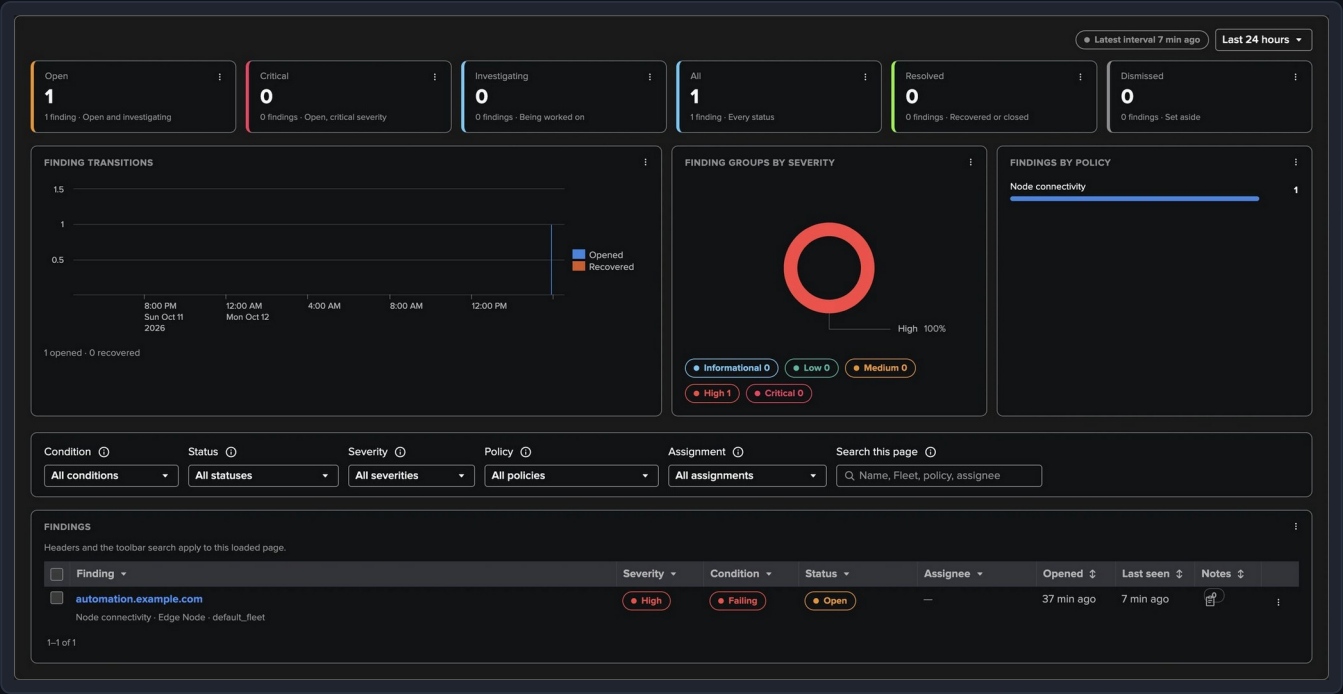
03

PART 3 • FINDINGS

Judged per Fleet, decided per group

The Findings tab, what you see when a node stops, the nodes that must stay connected, and version drift after a rollout.

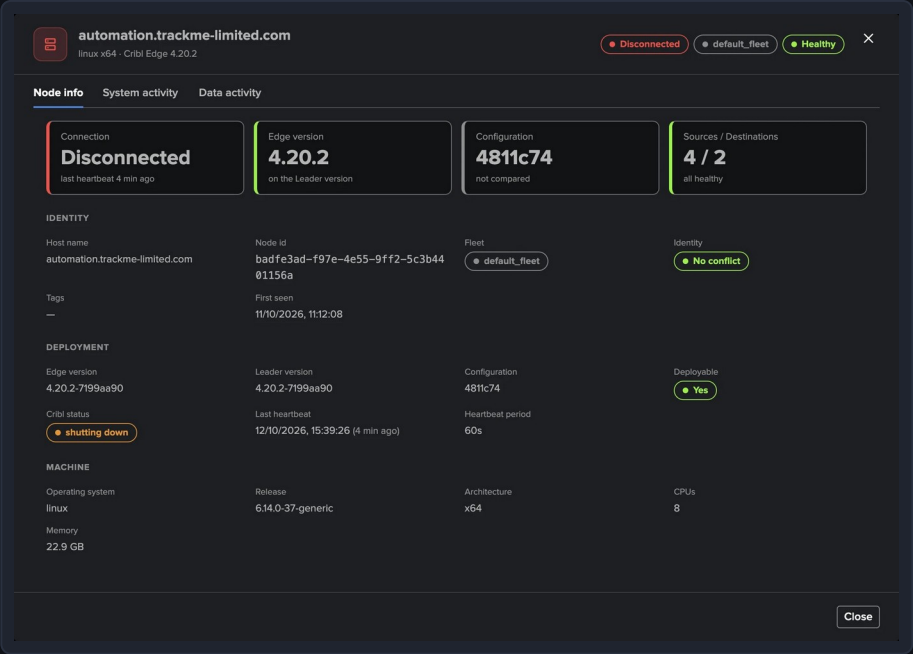
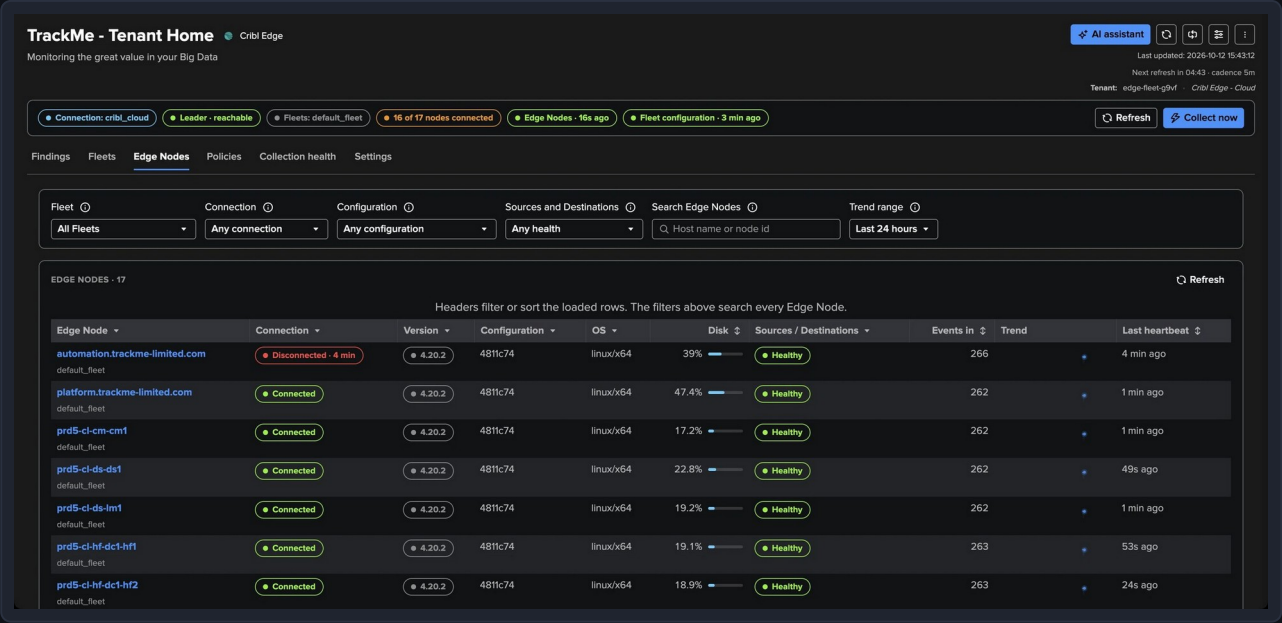
The Findings tab — the shared findings centre of the Cribl tenants



- 1 About a Fleet**
Connectivity, version and configuration drift, coverage, node identity.
- 2 About a Source or Destination**
Its health across the Fleet's nodes.

- 3 About an Edge Node**
Connectivity of selected nodes, disk, CPU, memory.
- 4 Open resource**
Opens the Fleet or the node the finding is about, in place.

A disconnected node — visible at once, a finding only when it matters



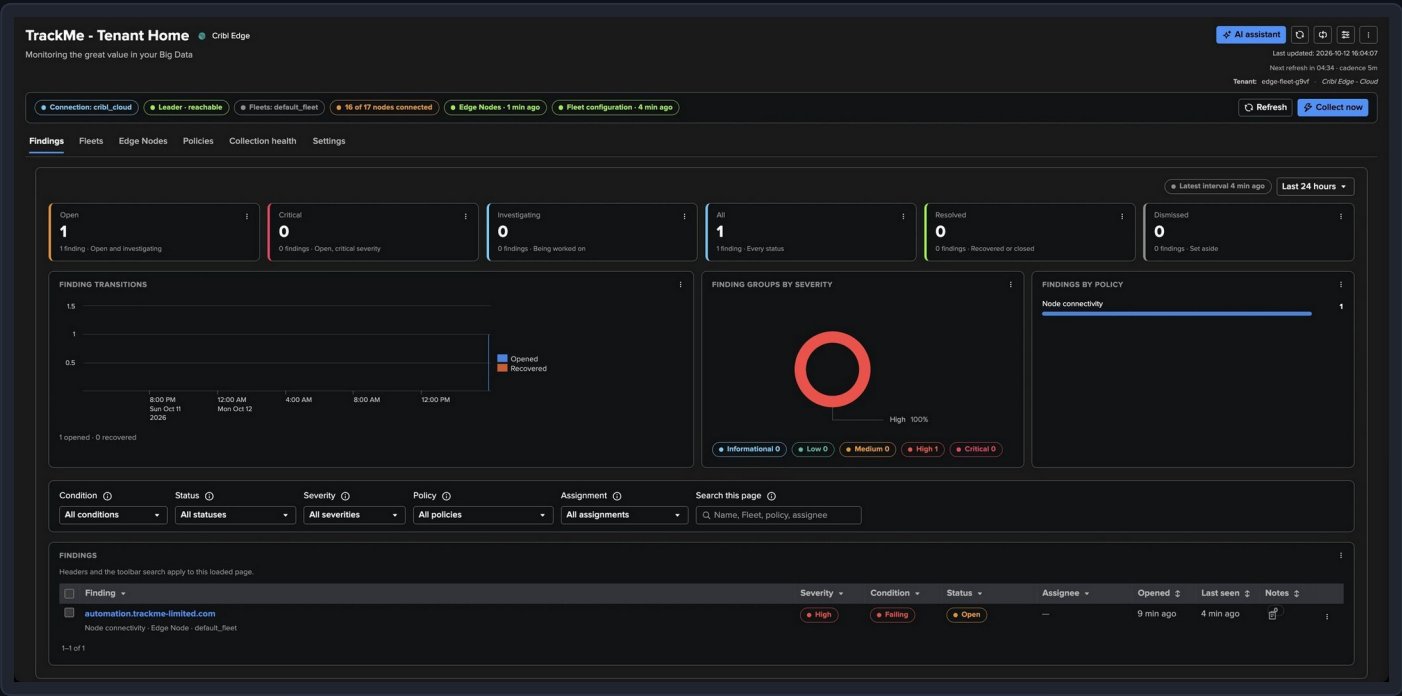
1 Within 10 minutes
16 of 17 nodes connected; the node listed as disconnected.

2 No finding for one node, by design
Fleet connectivity opens from 20 % of the Fleet and 2 nodes.

3 Nodes that must never drop
Select them in Node connectivity, typed or from a lookup: High after 15 minutes.

4 Dormant after 7 days
A retired node leaves the Fleet's count.

Node connectivity — a High finding about the node you selected



- 1 Selected nodes only**
Typed host names (dc-* accepted) or a Splunk lookup table.
- 2 High after three checks**
No heartbeat for 15 minutes.
- 3 Recovers when it reconnects**
Measured, not decided.
- 4 Quiet grey in Topology Studio**
A disconnected node without a finding is disclosed, not alarming.

Nodes that must stay connected — typed names, lookups, tested

Node connectivity

EnabledHigh

Edge Nodes · Selected nodes that must stay connected.

NODES THAT MUST STAY CONNECTED

Typed host names and the host names of Splunk lookup tables add up, case-insensitive. Typed names accept * for any text (dc-* selects dc-01.example.com). Long or changing lists belong in a lookup table: up to 500,000 host names each, read again every 15 minutes; a lookup that cannot be read keeps its last host names.

Host names

automation.trackme-limited.com

1 host name. One per line (spaces and commas also separate).

Lookup tables

Deployment	Lookup	Host name field	Match mode
Remote: prd5	example_cmdb_hosts	host	Exact

Add a lookup table

Each row of the field is a host name (or a pattern with *). Unreadable lookups are reported in Collection health; the other sources still apply.

Test selectionRuns as a search: reads the lookups now and matches the latest Edge Nodes directory. Saves nothing.

8 host names (8 exact, 0 with *) select 4 of 17 Edge Nodes: 3 connected, 1 disconnected, 0 unknown.

- 1

Typed host names

No count limit, case-insensitive; * stands for any text.
- 2

Splunk lookup tables

Up to 20, local or remote: 500,000 names each, Exact or Wildcard.

8 host names (8 exact, 0 with *) select 4 of 17 Edge Nodes: 3 connected, 1 disconnected, 0 unknown.

Each source and what it gave.

Source	Status	Names	Matching	Ignored
Typed host names	—	1	1	—
example_cmdb_hosts · host · exact (Remote: prd5)	Read	7	3	0

Selected Edge Nodes (up to 50, disconnected first)

Host name	Fleet	State	Matched by
platform.trackme-limited.com	default_fleet	disconnected	platform.trackme-limited.com
automation.trackme-limited.com	default_fleet	connected	automation.trackme-limited.com
uk1.trackme-limited.com	default_fleet	connected	uk1.trackme-limited.com
web01.trackme-limited.com	default_fleet	connected	web01.trackme-limited.com

4 host names select no Edge Node: akamai-hec-001.trackme-limited.com, eventgen-hec-001.trackme-limited.com, licenses.trackme-solutions.com, prd3-standalone

- 3

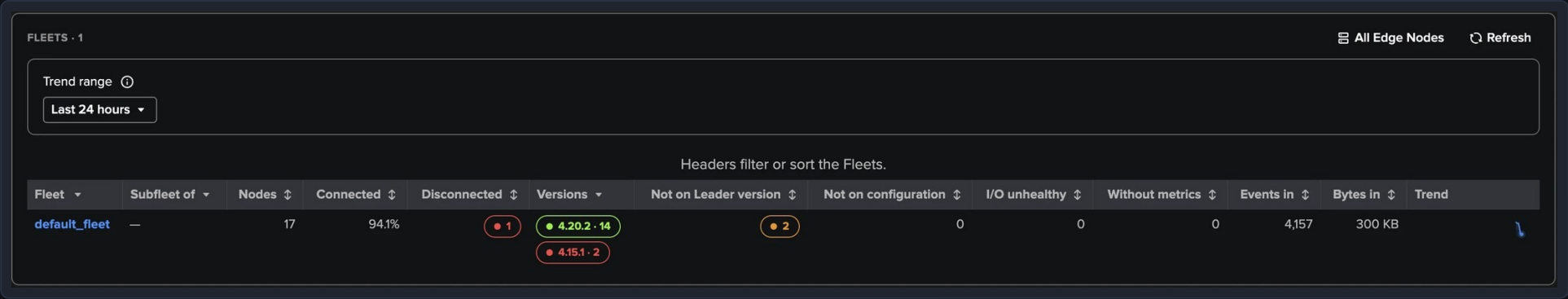
Read every 15 minutes

A lookup that cannot be read keeps its last good names.
- 4

Test selection

Runs as a search: which nodes, in which state, from which source. Saves nothing.

Version drift — the nodes an upgrade left behind



- 1

Baseline
The Leader version by default, or the Fleet's most common one.
- 2

Rollout grace
24 hours by default, the time of a rolling upgrade.

- 3

Medium, or High
High when a node is newer than the Leader or two minor versions behind.
- 4

Configuration drift
The same for deploys, after a 30-minute grace.

04

PART 4 • OPERATE

Rules you can explain

Eleven policies and bank holidays, collection health, settings, Topology Studio, the AI Assistant and the Cribl Edge AI Agent — and how Edge compares with Stream.

Eleven policies — eight on out of the box

POLICIES · 8 OF 11 ENABLED

A policy opens a finding when its condition holds and closes it once it recovers. Fleet policies judge each Fleet as a whole; node policies judge a node.

All 11

Cribl Leader 1

Fleets 6

Edge Nodes 4

Policy

Category

Status

Severity

Conditions

Scope

Actions

Leader availability

Cribl Leader

Enabled

Critical

No setting beyond severity and checks.

Configured Leader API

Edit

Fleet connectivity

Fleets

Enabled

High

Open at: 20% · Recover below: 10% · At least: 2 nodes · Critical at: 50% · Dormant after: 7 days

All Fleets

Edit

Version drift

Fleets

Enabled

Medium

Compare with: The Leader version · Rollout grace: 24 h · At least: 1 node

All Fleets

Edit

Configuration drift

Fleets

Enabled

High

Grace: 30 min · At least: 1 node · Critical at: 50%

All Fleets

Edit

Fleet coverage

Fleets

Enabled

Medium

Expected connected nodes: learned · Learned drop: 50%

All Fleets

Edit

Node identity

Fleets

Enabled

Low

Host name changes in 24 hours: 3

All Fleets

Edit

Source and Destination health

Fleets

Enabled

Medium

At least: 1 node · And at least: 0% · Critical at: 50% · Judge quiet Sources: no

All Fleets

Edit

Node connectivity

Edge Nodes

Enabled

High

Heartbeat older than: 15 min

1 host name patterns

Edit

Node disk

Edge Nodes

Disabled

High

Open at: 90% · Recover at: 85% · Critical at: 95%

All Fleets

Edit

Node CPU

Edge Nodes

Disabled

Medium

Open at: 90% · Recover at: 80%

All Fleets

Edit

Node memory

Edge Nodes

Disabled

Medium

Open at: 90% · Recover at: 80%

All Fleets

Edit

Node CPU

Edge Nodes · CPU used on a node over the last 10 minutes, from the Edge System Metrics forwarded to the tenant's System Metrics index (node_cpu_percent_active_all).

Disabled

Medium

POLICY

Enabled

Off

Severity

Medium

The severity of the findings this policy opens (a few policies raise it, as their settings say).

Checks to open

2

Consecutive failing checks (directory publications, every five minutes) before a finding opens.

Checks to recover

2

Consecutive healthy checks before an open finding recovers.

EDGE SYSTEM METRICS

This policy reads the System Metrics index **cribl_metrics_edge**: the node_* metrics of the Edge System Metrics source, matched to each node by its host name. A node without metrics there is not evaluated.

1. In Cribl Edge, turn on the **System Metrics** source of your Fleets (Basic level is enough).

2. Route its metrics to Splunk, directly or through Cribl Stream, into a Splunk **metrics** index. Keep the metric names (node_cpu_percent_active_all, node_memory_Used_percent) and the host dimension, the node's host name.

3. In this tenant's Settings, Source and Fleets, select that index as the **System Metrics** index.

Each policy run reads the index once for every node (the average of the last 10 minutes); no node is read one by one, whatever the Fleet size. Node disk needs nothing of this: the disk comes with every heartbeat.

Close

Save policy

1 Cribl Leader, Fleets, Edge Nodes
Three categories, as cards or a list.

2 Node disk, CPU and memory off
Node resources are a choice: a fleet of endpoints would flood on day one.

3 Needs nodes / Needs System Metrics
Pills tell what a policy waits for.

4 Editor
On or off, severity, checks, conditions, scope, bank holidays.

TrackMe for Splunk · Hands-on: Cribl Edge

docs.trackme-solutions.com

Bank holidays — each policy decides whether a holiday holds it

<-->

Fleet connectivity

Enabled

High

×

20

^

▼

A finding opens when this share of the Fleet's active nodes is disconnected.

Recover below (%)

10

^

▼

The finding recovers once the share falls below this value.

At least (nodes)

2

^

▼

Never open for fewer disconnected nodes than this, whatever the share.

Critical at (%)

50

^

▼

The finding is critical from this share (or when no node is connected).

Dormant after

7 days

▼

A node disconnected for longer leaves the Fleet's count (It is listed apart as dormant).

BANK HOLIDAYS

During bank holidays

Hold new findings

While a bank holiday of this tenant's calendars is active and the tenant suppresses new alerts on holidays (Manage Bank Holidays), this policy opens no new finding. A finding already open is still evaluated and can recover.

SCOPE

Fleets

Select...

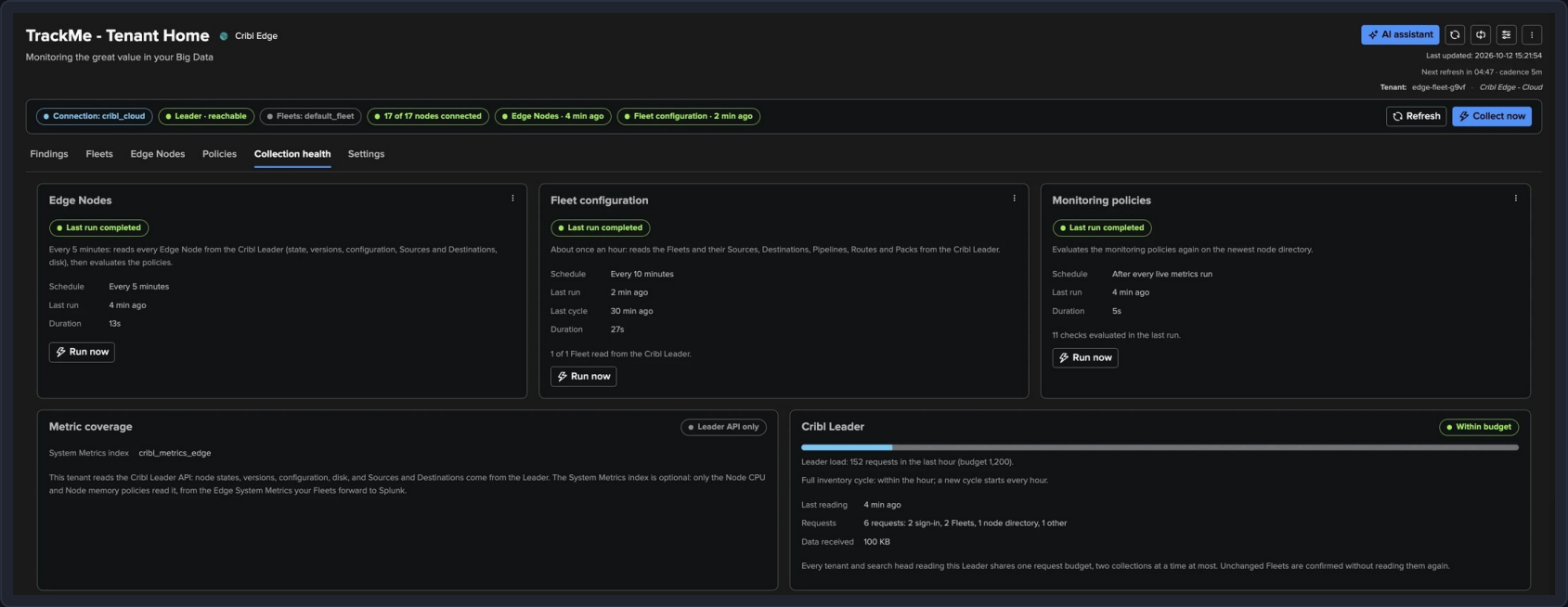
Empty: every Fleet of the tenant.

Close

Save policy

- 1 The tenant's calendars**
The system defaults, its own or none, in Manage Bank Holidays.
- 2 One effect for Edge**
Suppress new alerts. No ML to keep holidays from, no SLA.
- 3 Per policy**
During bank holidays: Hold new findings, or Keep opening findings.
- 4 Held by default**
Fleet connectivity and Fleet coverage: endpoints switched off for the holiday.
- 5 Kept by default**
Node connectivity and every other policy. Leader availability is never held.
- 6 Open findings go on**
Still evaluated during the holiday: they can recover and close.

Collection health — two jobs and the Leader budget



- 1

Edge Nodes

Every 5 minutes: the node directory, then the policies.
- 2

Fleet configuration

About once an hour.
- 3

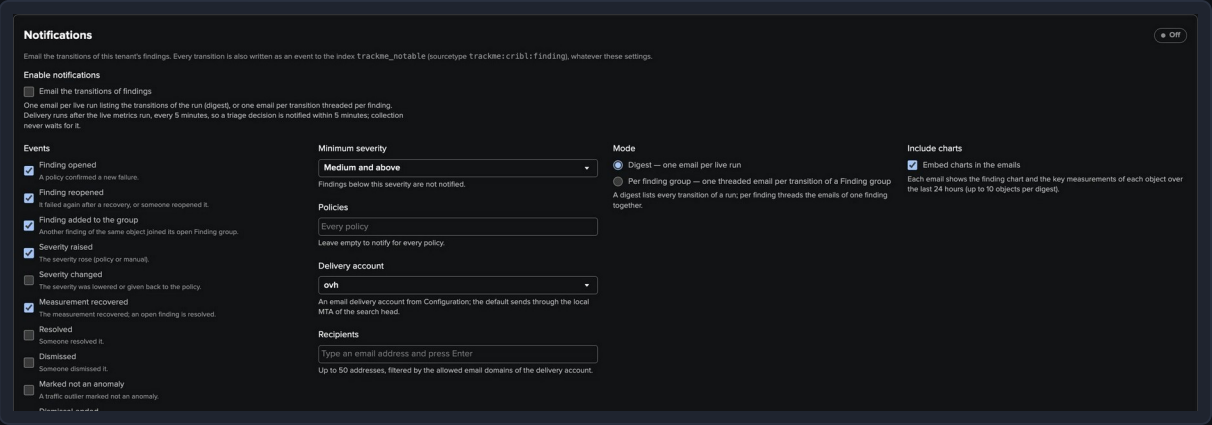
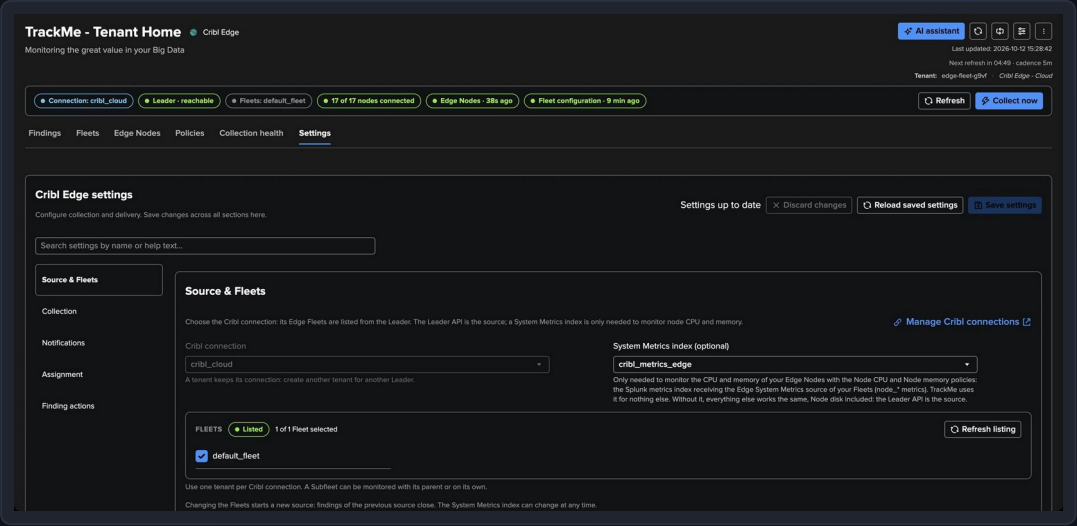
Leader requests

The load against the connection's budget.
- 4

Guardian

cribl_collection_health, with the Edge conditions.

Settings — one Save for every section

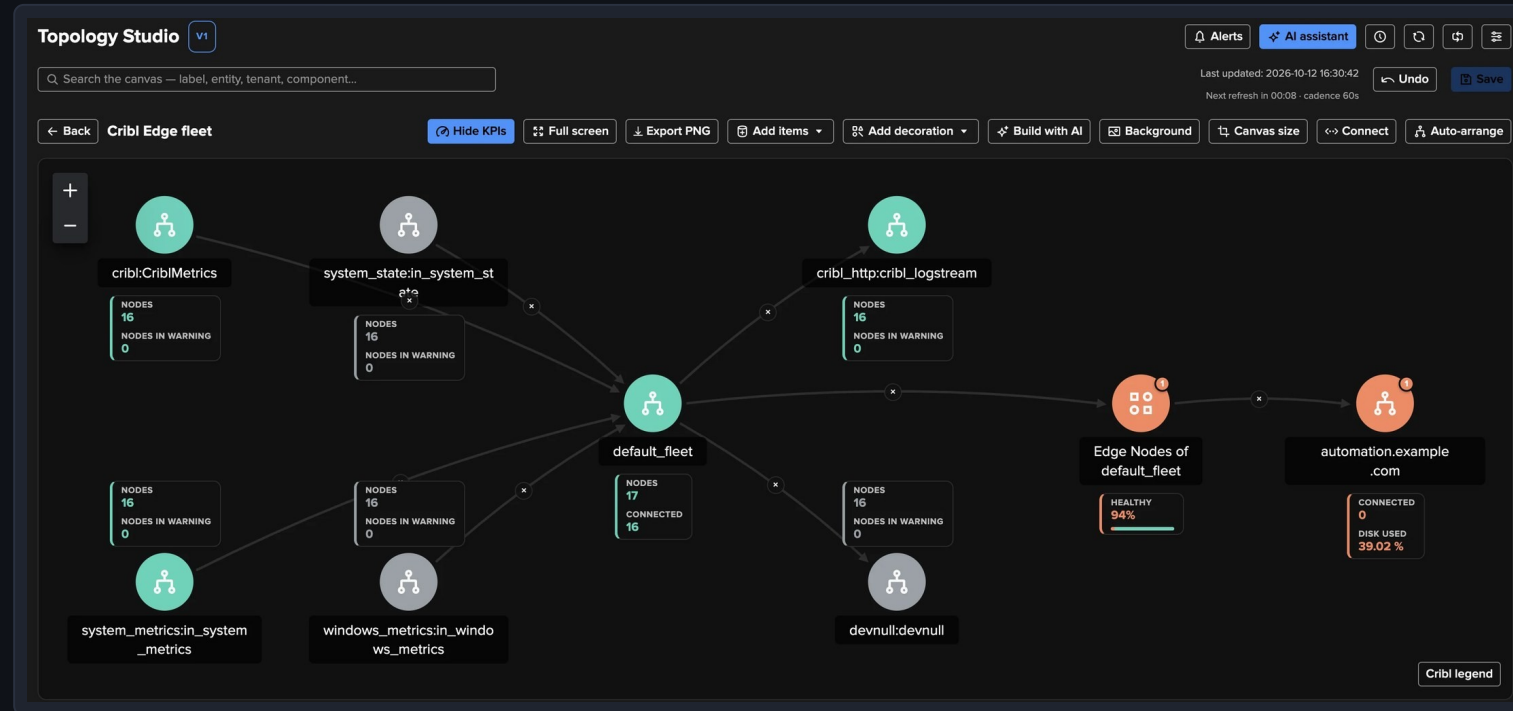


1 **Source & Fleets**
Locked connection, the Fleets, the System Metrics index, Repair workspace.

2 **Notifications**
Events, minimum severity, delivery account, digest or per group, charts.

3 **Assignment and Finding actions**
Groups, routing rules, drilldowns, links, webhooks, automations.

Edge in Topology Studio — groups that follow the fleet



Add an aggregate node

A Cribl aggregate either follows a selection (object types, Worker Groups or Fleets, a name): objects that start matching join it and removed ones leave it, or holds the objects you choose. Its colour follows the open findings of its members.

Node label *

Edge Nodes of default_fleet

Scope * 1 of 8 tenant < component pairs

edge-fleet-g9vf ▼

Remove

Chosen objects

Follow a selection

Start from

Edge Nodes of a Fleet

Disconnected Edge Nodes

Edge Nodes by host name

Fleets

Sources and Destinations

Everything with a finding

What

☐ Fleets (1)

☐ Sources (4)

☐ Destinations (2)

☒ Edge Nodes (17)

Where

default_fleet X

Name contains

Host name, Fleet or Source / Destination id,

Connection

Any connection

Version

Any version

Configuration

Any configuration

Sources / Destinations health

Any health

☐ Only objects with open findings

☒ 17 Edge Nodes in 1 Fleet, 1 with open findings

Cancel

Add aggregate

- 1

Fleets, Sources, Destinations, Edge Nodes
Picked with the Edge Nodes filters.

2

Groups
Edge Nodes of a Fleet, disconnected nodes, everything with a finding.

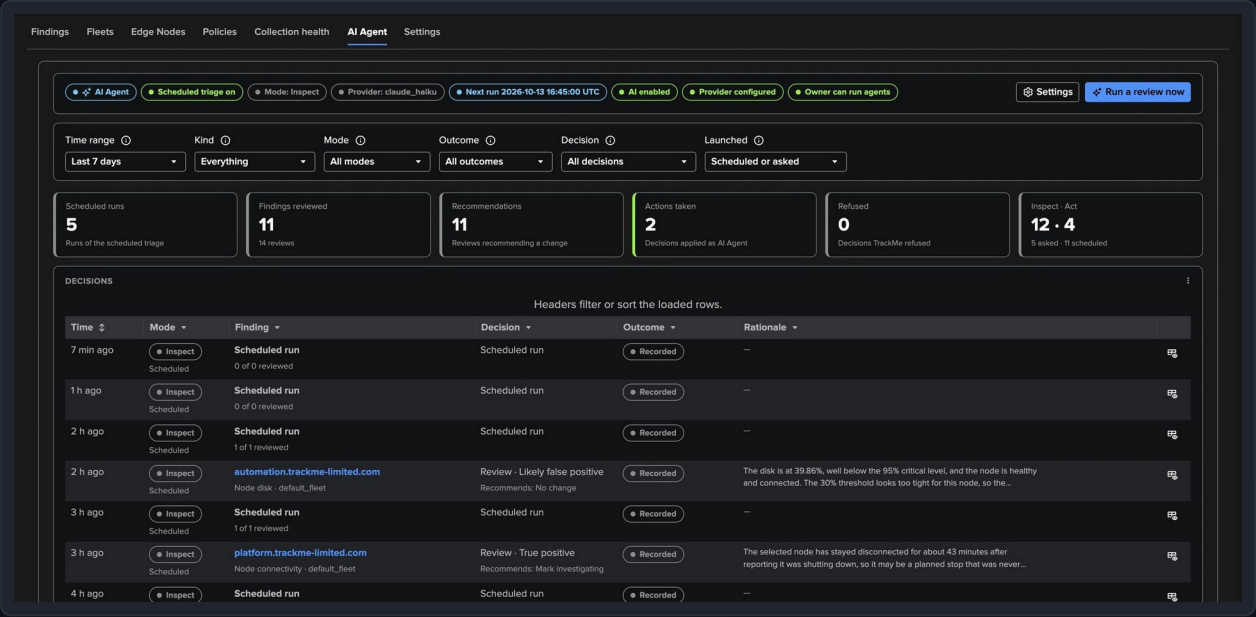
3

Status
Findings first; a disconnected node without a finding is quiet grey.

4

Create with AI
Fleet overview, Edge problems wall, Sources and Destinations of a Fleet.

The Cribl Edge AI Agent — triage by an agentic operator



- 1

Reviews like an operator

From the facts TrackMe holds: no search, no call to Cribl, no ML.
- 2

Five assessments

True positive, likely false positive, expected, not in use, needs investigation.
- 3

Inspect, then act

Mark investigating, dismiss for a time, resolve on a measured recovery.
- 4

Only what the tenant allows

Each decision has its setting; TrackMe re-checks it before applying.
- 5

Hourly scheduled triage

Never over an operator's decision; one current [AI Agent] note.
- 6

Every decision logged

The AI Agent tab: runs, reviews, actions taken, refusals.

Custom instructions — and Evaluate before they run

ALLOWED ACTIONS

What the agent may apply in act mode. Inspect runs only recommend, and the agent never dismisses permanently, assigns, changes a severity, a policy or the Fleets the tenant collects.

Mark Investigating

Sets an open finding to investigating, with the rationale in its history. Nothing else changes.

Dismiss for a time

Dismisses the finding for a few days at most. It returns to the open list when that time ends, or at once if reopened. A critical or high finding that is still failing is dismissed only when its node or Fleet is no longer in the node directory.

Longest dismissal (days)

7

The longest dismissal the agent may set, 1 to 90 days.

Resolve

High Impact - off by default

Resolves a finding whose measurement has recovered. A new failure opens it again.

CUSTOM INSTRUCTIONS

Evaluate...

Plain English the Cribl Edge AI Agent follows on every run of this tenant, asked or scheduled: what to treat as expected, what to look at first, how to word its recommendations. They never widen what it may do: the allowed actions above and the checks TrackMe makes before every decision still decide.

The nodes whose host name starts with prd5-cl-idx are lab indexers: their disk usage between 50% and 80% is expected. Word every rationale in two short sentences for the on-call engineer.

187 / 4000 characters

Evaluate runs the agent in inspect mode with this text, saved or not, on one finding or the open findings, and shows what it would say. It writes nothing.

Evaluate custom instructions

Cribl Edge AI Agent

Inspect - writes nothing

Saved

Evaluation: nothing is written (no note, no decision). The agent reviews in inspect mode, following the instructions below in place of the saved ones, and only shows what it would say.

INSTRUCTIONS EVALUATED

The nodes whose host name starts with prd5-cl-idx are lab indexers: their disk usage between 50% and 80% is expected. Word every rationale in two short sentences for the on-call engineer.

These are the saved instructions: every run of the agent follows them.

Finding: prd5-cl-idx-dc1-idx2

WITH THESE INSTRUCTIONS

The agent follows the instructions evaluated.

Attention

SUMMARY

The node disk finding on prd5-cl-idx-dc1-idx2 is failing at 68.91% used, above the 30% policy threshold but well below the 95% critical level. The host name starts with prd5-cl-idx, so per the tenant's custom instructions this lab indexer's usage between 50% and 80% is expected. No decision is recommended: dismiss_temporary is refused (critical_failing, the node is still in the directory), resolve is not allowed while the measure is failing, and the threshold itself is an operator decision.

WITHOUT CUSTOM INSTRUCTIONS

The same review with no custom instructions, for comparison.

Attention

SUMMARY

One finding reviewed in inspect mode, no decision applied. The Node disk finding on prd5-cl-idx-dc1-idx2 is a real, still-failing condition: disk is at 68.91% against a policy threshold of 30% (recovery at 20%, critical at 95%). The node is connected, healthy and in a current directory. Recommend investigating: dismissal and resolve are not allowed by the server.

FINDINGS ASSESSED (1)

Expected Behaviour

prd5-cl-idx-dc1-idx2

Node disk

High confidence

Decision: No change

Evidence: Disk used is 68.91 percent against a 30 percent threshold and a 95 percent critical level, with the node connected, healthy and in a current directory. The host name prefix prd5-cl-idx marks it as a lab indexer, and the custom instructions say 50 to 80 percent is expected for these nodes. A dismissal is refused because the high finding is still failing with the node in the directory.

The disk usage falls in the 50-80 percent band the tenant treats as expected for lab indexers. No decision is possible here since dismiss_temporary is refused (critical_failing) and resolve is not allowed while failing; operators may want to tune the

True Positive

prd5-cl-idx-dc1-idx2

Node disk

High confidence

Decision: Mark Investigating

Evidence: Disk used is 68.91% (policy threshold 30%, recovery 20%, critical 95%), failing for 2 buckets, episode 1, opened 1791891600, high severity. The node is connected, status healthy, Edge 4.20.2 matching the Leader, and the directory is current (age 205 s), with no collection problems. Measurement is still failing, so resolve is not allowed; dismiss_temporary is refused because the finding is high and failing with the node still in the directory.

Disk on this indexer is above the policy threshold and has not recovered, so someone should look at log retention, index sizing or volume growth. It is well below the 95% critical level, so the severity is not an emergency. The existing AI note mentions a 50% threshold, but the policy evidence shows 30%; the operators should confirm the

Close

Evaluate again

- 1

Plain English, per tenant

What is expected here, what to look at first, how to word it.
- 2

Never widen its power

The allowed decisions and TrackMe's checks still decide.

- 3

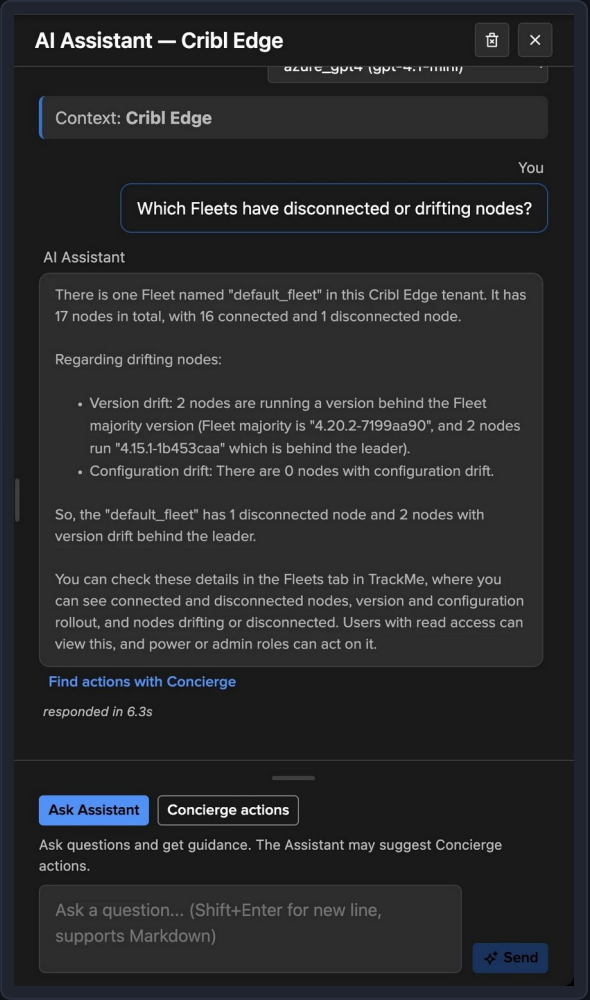
Evaluate

The same review with and without your text, side by side. Writes nothing.
- 4

Here

Lab indexers at 50–80 % disk: Expected behaviour instead of investigating.

The AI Assistant, and Edge next to Stream



	Cribl Stream	Cribl Edge
Main source	Cribl metrics in Splunk + Leader API	Leader node directory (+ System Metrics)
Policies	16, 14 on	11, 8 on
Judgement	Per object, traffic ML models	Per Fleet, selected nodes, thresholds
Size of one tenant	About 20 000 objects	Any fleet size
AI	Assistant, Concierge, AI Agent	Assistant, Cribl Edge AI Agent
Findings model	Shared	Shared

Where we are

In four parts

● Set up

a tenant on the Edge Leader, its Fleets selected, an optional System Metrics index

● Followed

Fleets and Edge Nodes from the directory, one node up close with System activity

● Judged

a disconnected node and version drift, per Fleet and per selected node

● Operated

policies and bank holidays, collection health, settings, Topology Studio, the assistant and the AI Agent

What made it work

One bulk read, any size

The node directory read page by page: no call per node, no node limit, every node current within five minutes.

Judged like an operator would

Shares of a Fleet, graces and selected nodes: one sleeping laptop opens nothing, a fifth of a Fleet does.

Detail on demand

A node's system activity and live Source status read only when someone opens it.