HANDS-ON WALKTHROUGH · SPLUNK FORWARDER COLLECTORS

Is every input of your collection points collecting?

One tenant follows the forwarders a Splunk deployment uses as collection points — add-on collectors and syslog collectors — from what Splunk already writes: their metrics.log, splunkd.log, introspection and configuration changes.

Captured live on TrackMe 2.4.24 · two add-on collectors (DB Connect, Okta, JMX, GitHub) and two syslog collectors (universal forwarders 9.4 and 10.6)

THE PROBLEM

A collector that keeps running can still collect nothing

A database password expires, an API token is revoked, a syslog feed stops: the forwarder stays green, and the data is missed days later.

Inputs that fail

A process stopped or crashing, errors in its own log, an input disabled that must stay enabled.

Feeds that go quiet

A source or a syslog feed with a rhythm of its own that stops.

Collectors in trouble

Silent, output blocked, pipeline saturated, disk filling, a group below its minimum.

What a Splunk Forwarder Collectors tenant does

Every input as configured, for any add-on, with two separate answers: does it run, and does it work. Nothing to install on a collector, no new data: TrackMe reads what Splunk already writes. Twenty-eight built-in policies judge the collectors, their inputs, the groups and the fleet, and the destinations.

THE MODEL

An input is what you configured — a process is what runs

1 Source

metrics.log, splunkd.log, introspection and _configtracker of each collector.

2 Directory

Collectors and utility nodes; declared syslog collectors; groups.

3 Inputs

Named by an API account, a configuration change, or what they deliver.

4 Decide

28 built-in policies on collectors, inputs, groups, fleet and destinations.

5 Act

Finding groups, notifications, findings actions, the AI Agent, the Fleet map.

Input states

Delivering, Logging, Running or Writing, its process runs, Disabled, or No activity evidence — never a failure on its own: a daily input between two runs reads that way.

Syslog and file collectors are declared: nothing in Splunk says a forwarder collects other machines' files, so you say it on a group.

THE PLAN

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

PART 1

Setup

- The wizard and the discovery
- Groups, two syslog collectors declared
- A least-privilege owner

PART 2

Configure

- Groups and their minimum
- Inputs that must stay enabled
- Notifications

PART 3

Follow

- Collectors, inputs, processes
- One collector up close
- Inventory and policies

PART 4

Findings

- A group below its minimum
- One Finding group per object
- The Fleet map

Every screen is the product as shipped, on four collection points of one Splunk deployment.

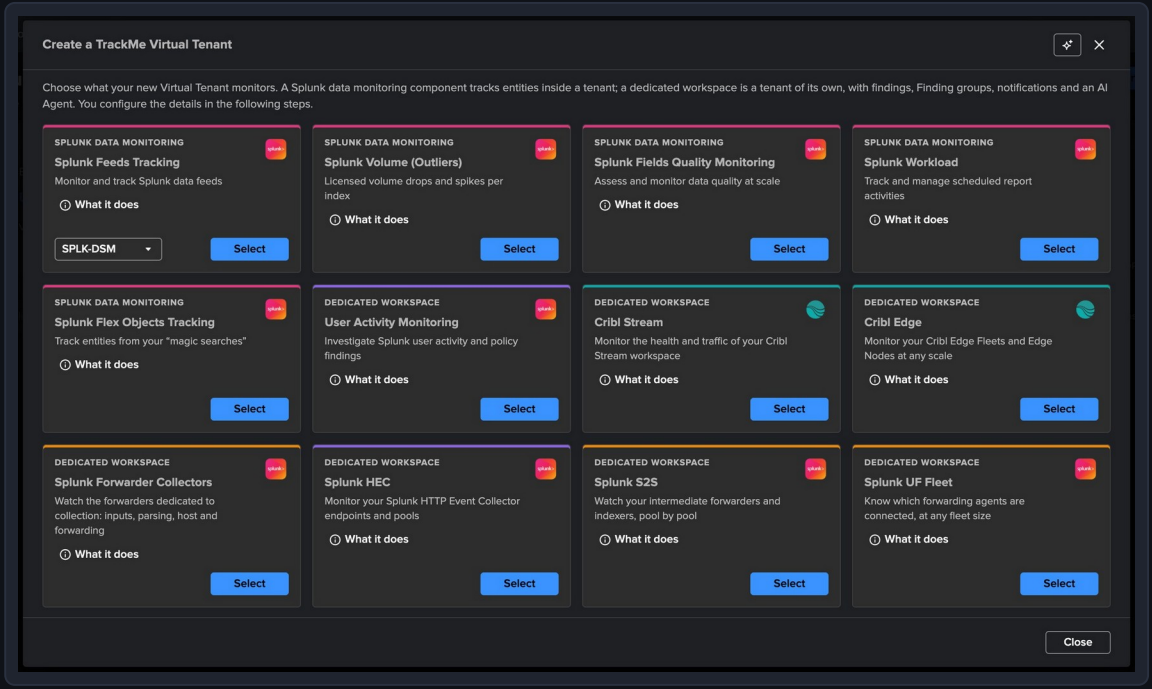
01

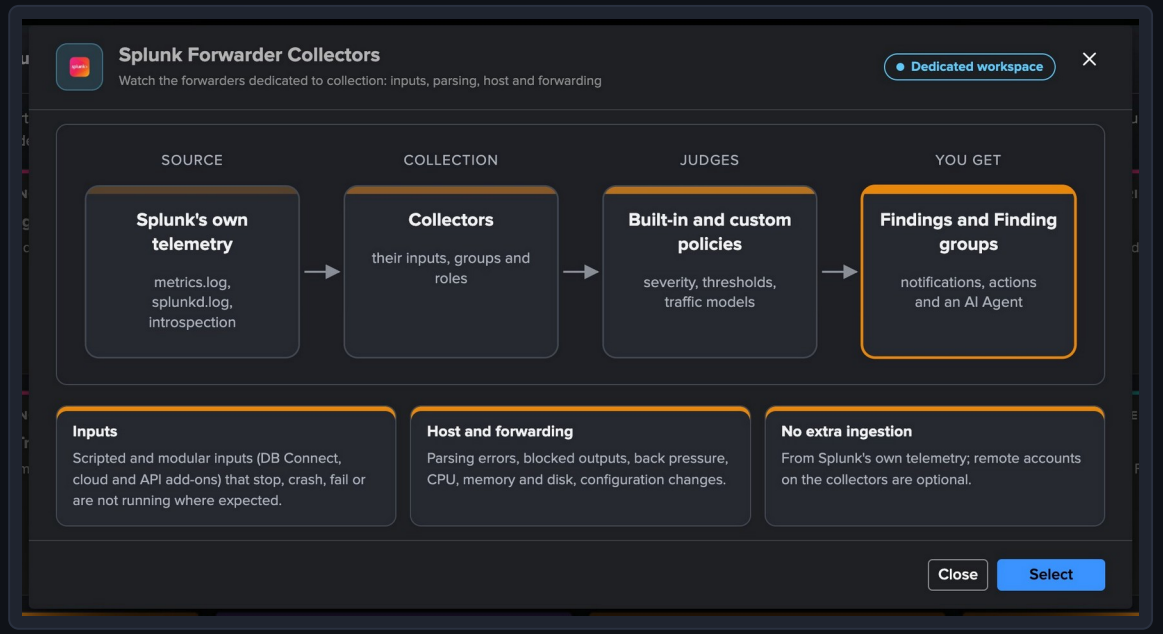
PART 1 · SETUP

One source, four collection points

The Splunk Forwarder Collectors card, the collector API accounts, the discovery and the groups, with two syslog collectors declared.

A dedicated tenant — pick Splunk Forwarder Collectors





1 The card

Watch the forwarders dedicated to collection: inputs, parsing, host and forwarding.

2 What it does

Splunk's own telemetry, the collectors, built-in and custom policies, findings.

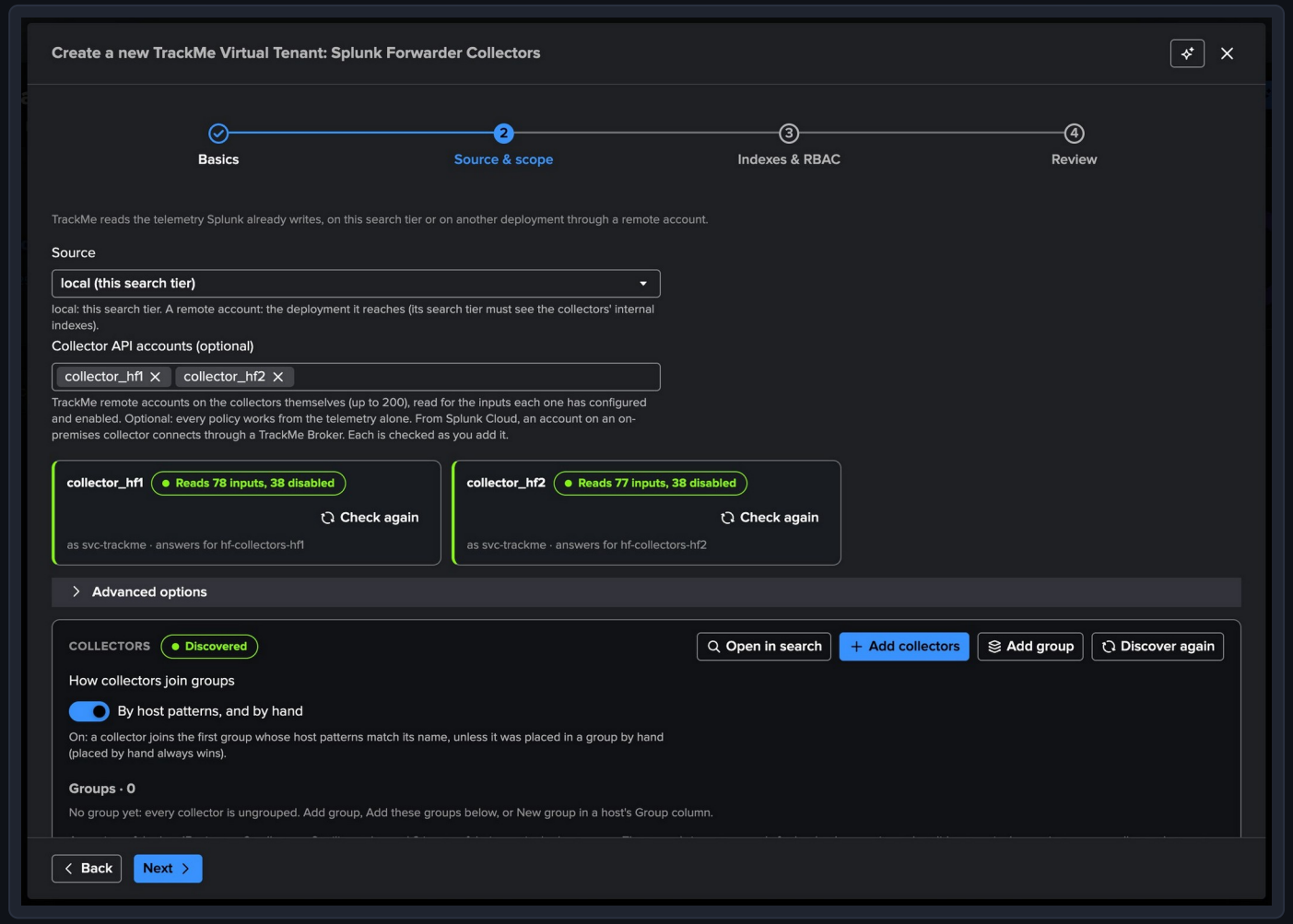
3 Four steps

Basics, Source & scope, Indexes & RBAC, Review.

4 Licence

Enterprise, Unlimited, the Unlimited trial or Developer.

Source and collector API accounts — the API is optional



1 **Source**

Where the collectors' internal indexes are searched: local here.

2 **Collector API accounts**

Optional: the current list of each collector's inputs and their state.

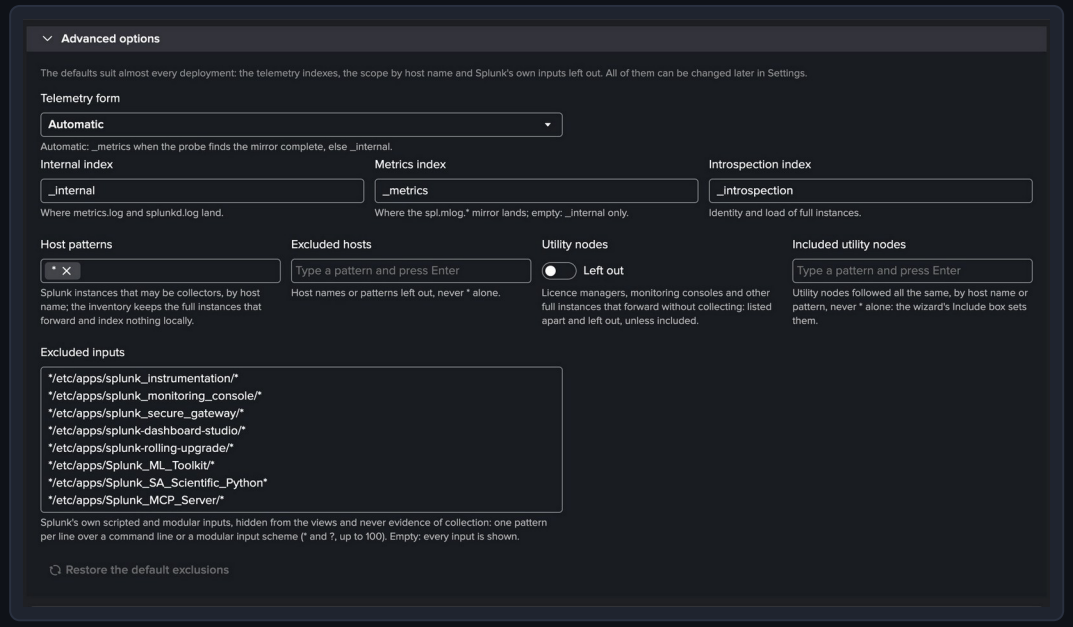
3 **Never required**

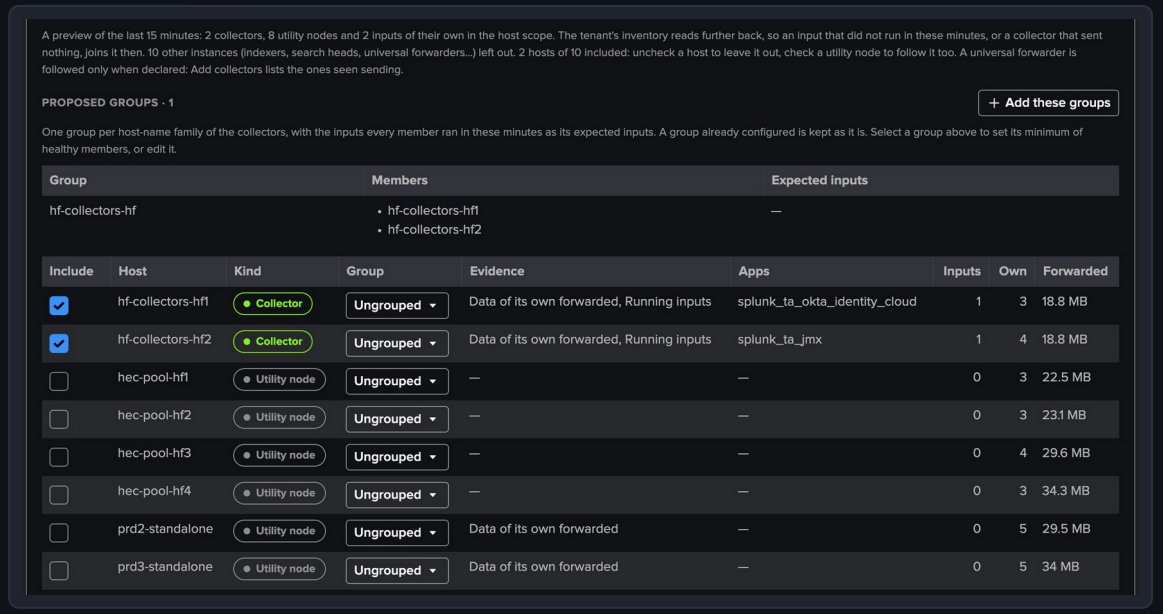
Every policy works from the telemetry alone; from Splunk Cloud, an account on an on-premises collector connects through a TrackMe Broker.

4 **The Collectors card**

How collectors join groups, the groups, Add collectors and Add group, then the discovery.

Scope, Splunk's own inputs left out, and a proposed group





1 Host patterns

The instances that may be collectors; excluded hosts never read.

2 Utility nodes

Licence managers, monitoring consoles: listed apart, left out unless included, all or one by one.

3 Excluded inputs

Splunk's own scripted and modular inputs, never evidence of collection.

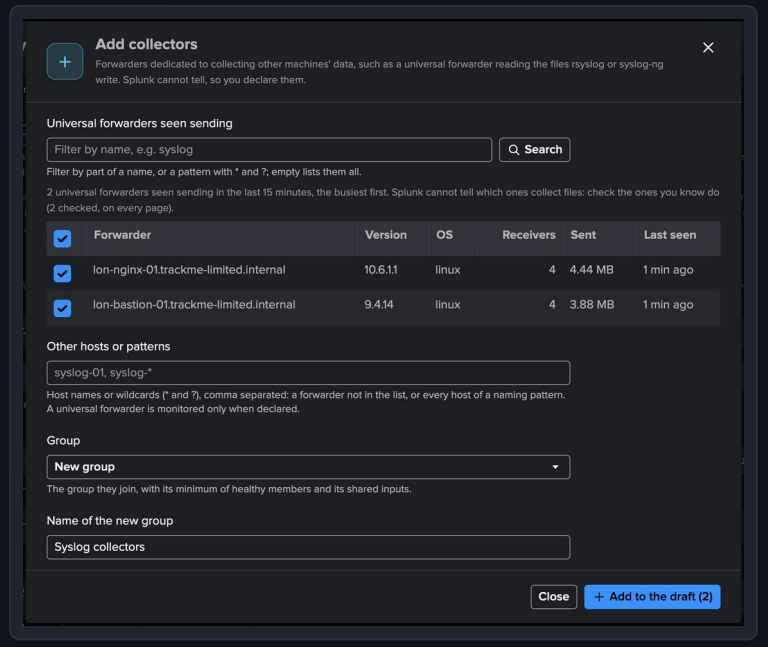
4 Include

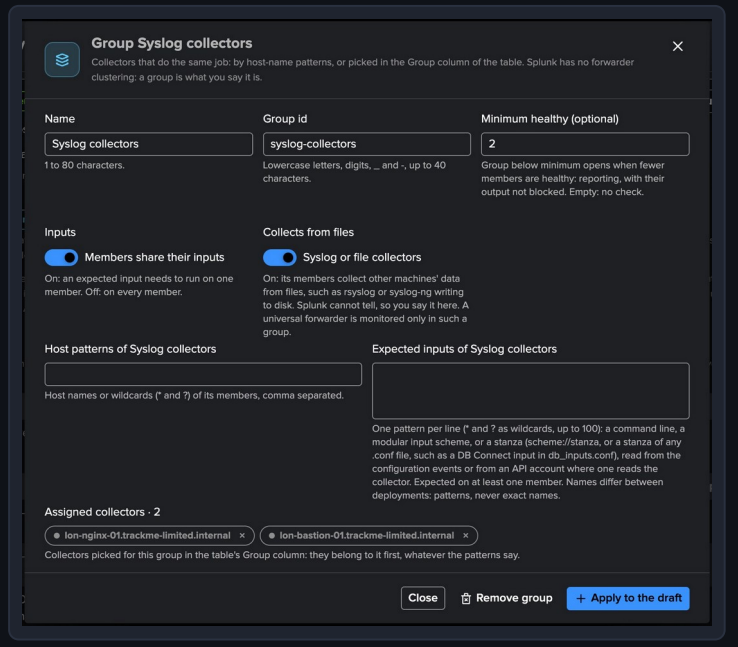
Uncheck a collector to leave it out, check a utility node to follow it.

5 Group column

Place a host in a group by hand, or in a new group; Add these groups takes the proposal.

Syslog and file collectors — declared, never detected





1 **Add collectors**

The universal forwarders seen sending, the busiest first: two that monitor the files rsyslog writes, into a new group.

2 **Syslog or file collectors**

Splunk cannot tell, so you say it: a universal forwarder is monitored only then.

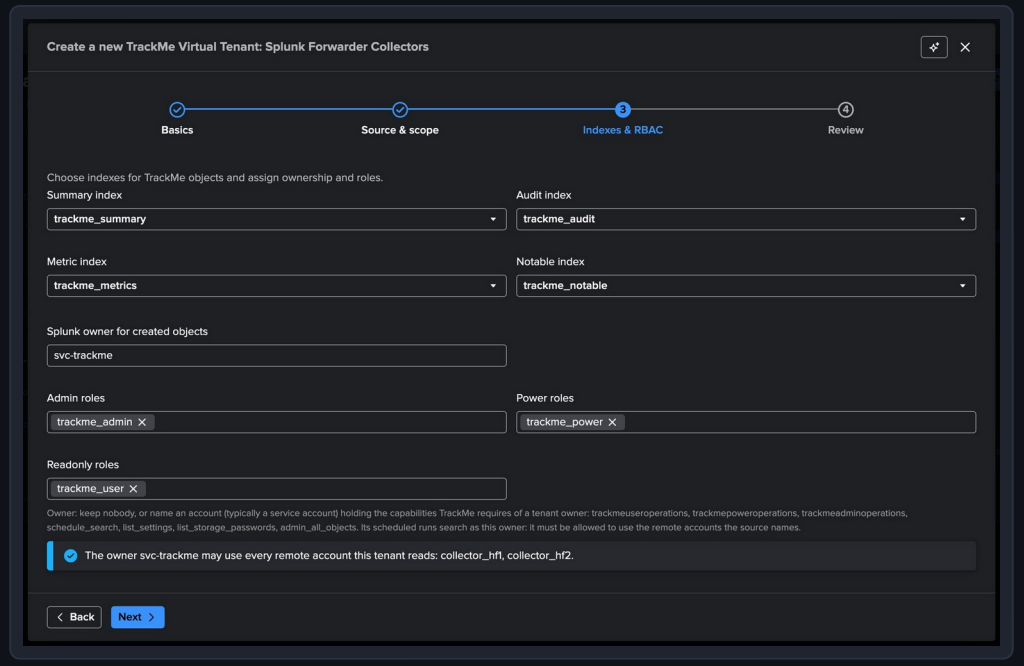
3 **Minimum healthy: 2**

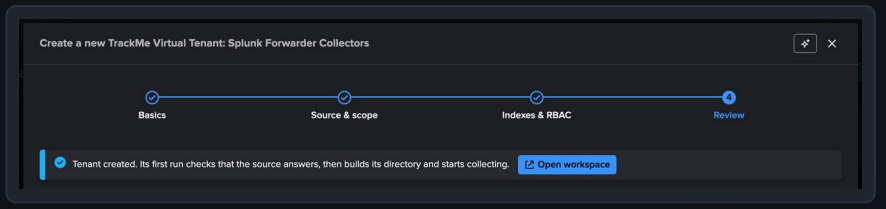
Group below minimum opens when fewer members report with their output not blocked.

4 **Members share their inputs**

Both monitor the same files: an expected input needs one member.

A least-privilege owner — checked before the tenant exists





1 Tenant owner

svc-trackme, a least-privilege service account: the scheduled runs search as it.

2 Remote accounts

The wizard checks the owner may use collector_hf1 and collector_hf2.

3 Done

The first run checks the source, builds the directory and starts collecting.

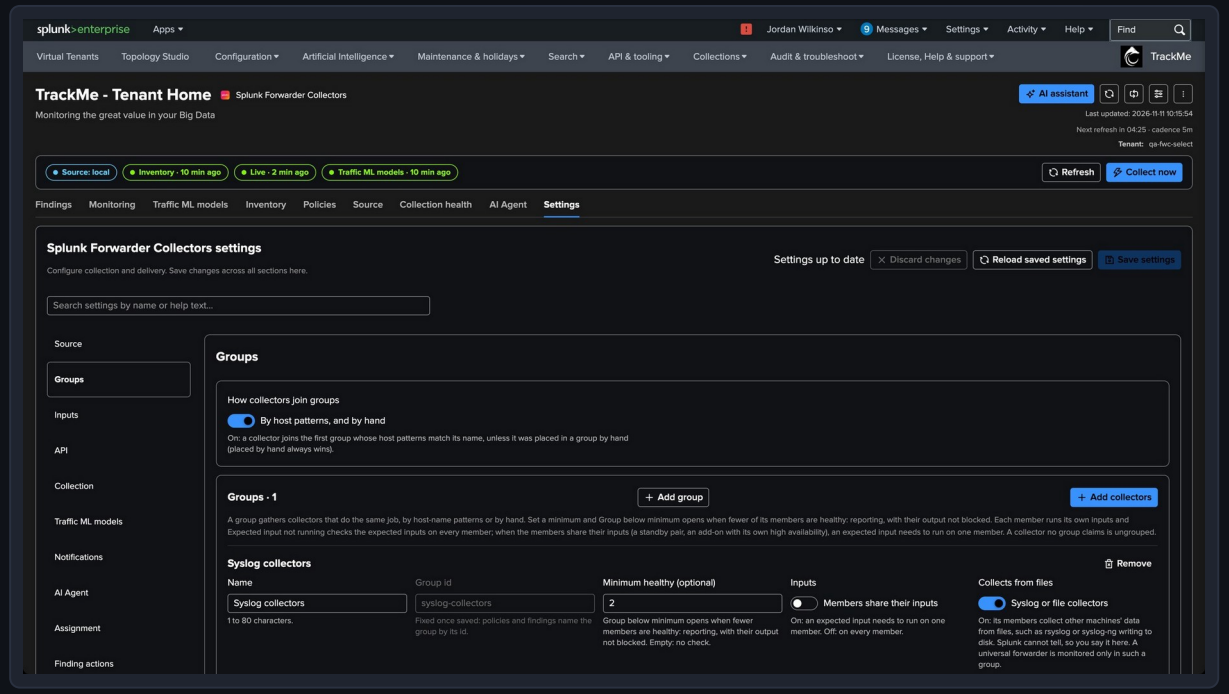
02

PART 2 · CONFIGURE

Groups, inputs that must stay enabled, notifications

The groups and their minimum, the inputs an add-on must never disable, and the emails of the findings.

Groups — collectors that do the same job



1 **How collectors join groups**

By host patterns and by hand, or by hand only.

2 **Syslog collectors**

Minimum 2, inputs shared, syslog or file collectors on.

3 **Expected inputs**

A command line, a scheme or a stanza, with wildcards.

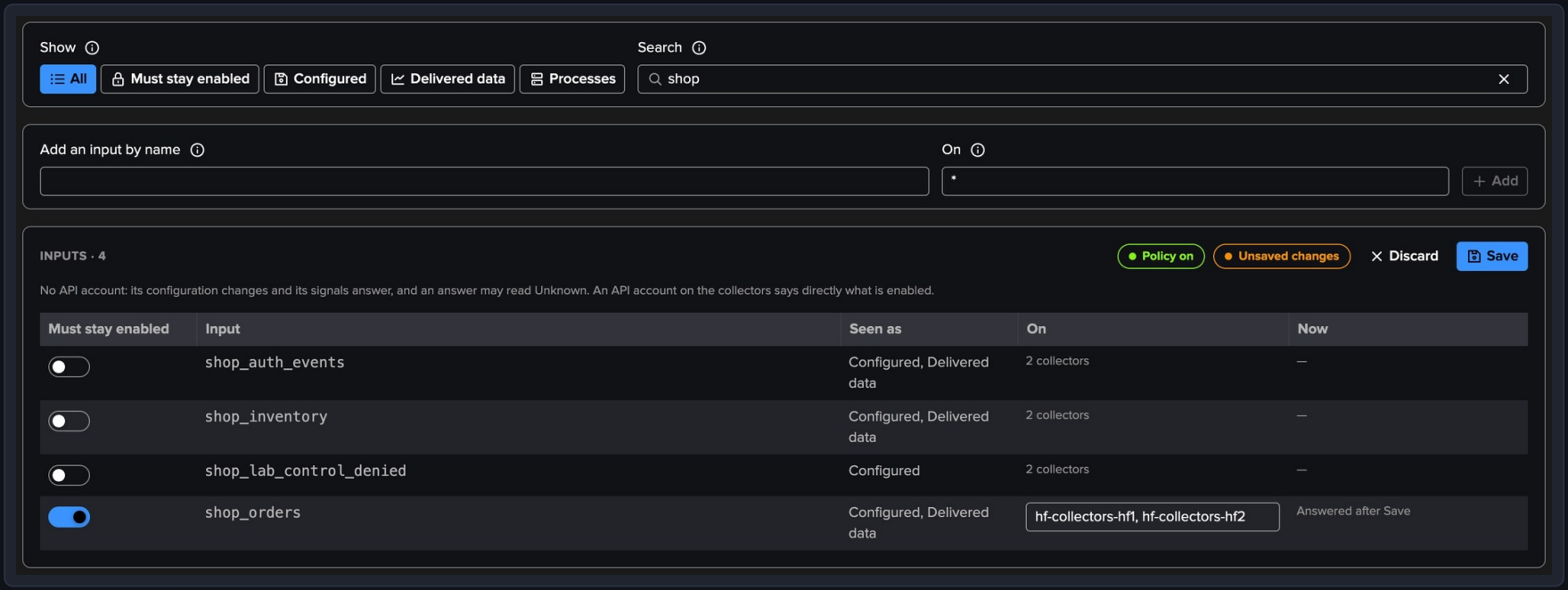
4 **Add collectors**

The same dialog as the wizard, also in the Inventory.

5 **The id is fixed**

Findings and history follow it.

Inputs that must stay enabled — a draft until Save



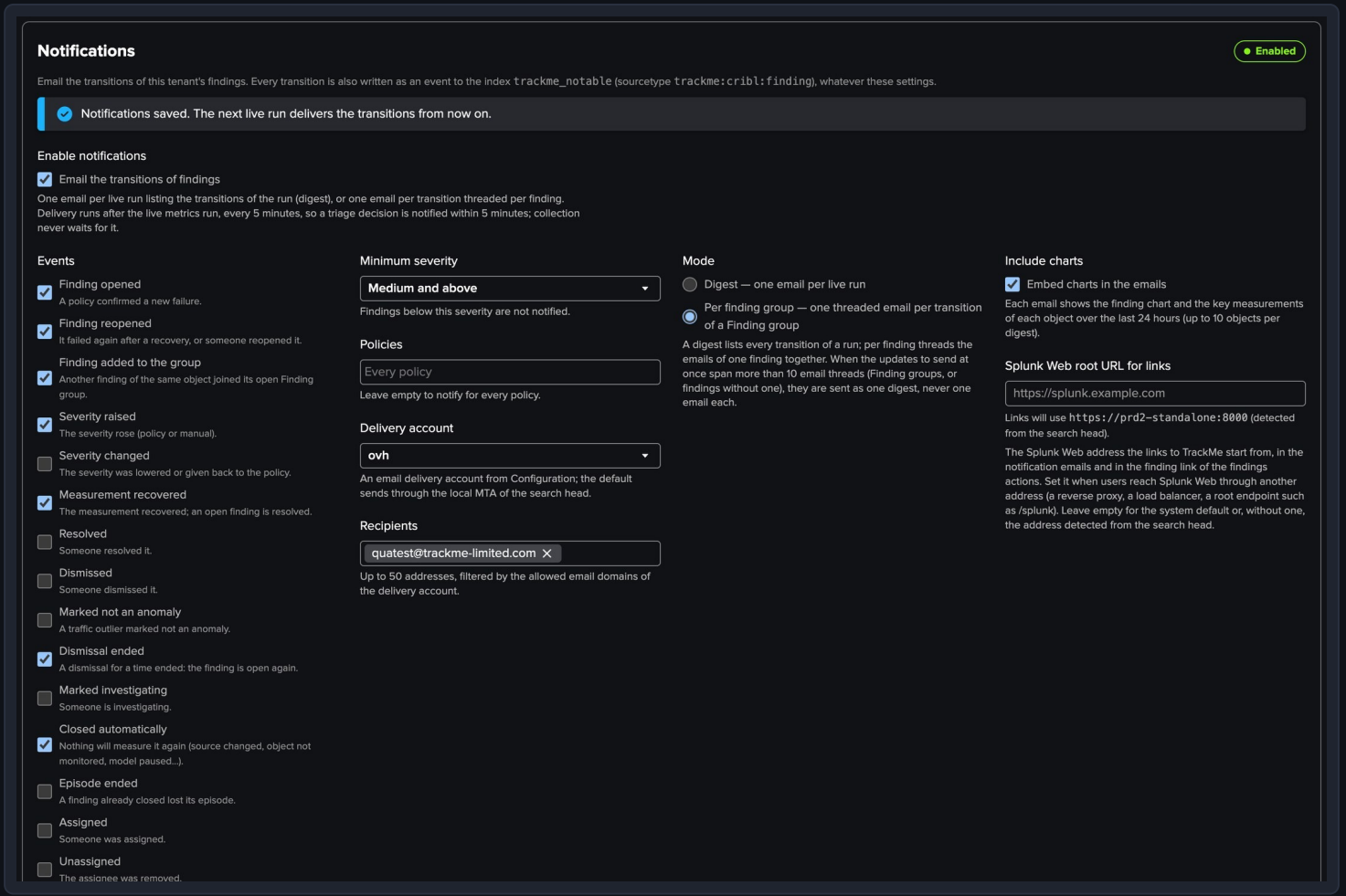
1 **Every input seen**
Configured, delivering data, or as a process.

2 **A switch per input**
shop_orders must stay enabled on both add-on collectors.

3 **Draft, Discard, Save**
Answered after Save, on the collectors named.

4 **Why**
DB Connect disables an input after repeated connection failures.

Notifications — one threaded email per Finding group



1. **Events**
   Opened, reopened, added to the group, severity raised, recovered...

2. **Minimum severity, policies**
   Medium and above, every policy.

3. **Delivery account, recipients**
   An email delivery account and up to 50 addresses.

4. **Mode and charts**
   Per Finding group, threaded; the finding's chart embedded.

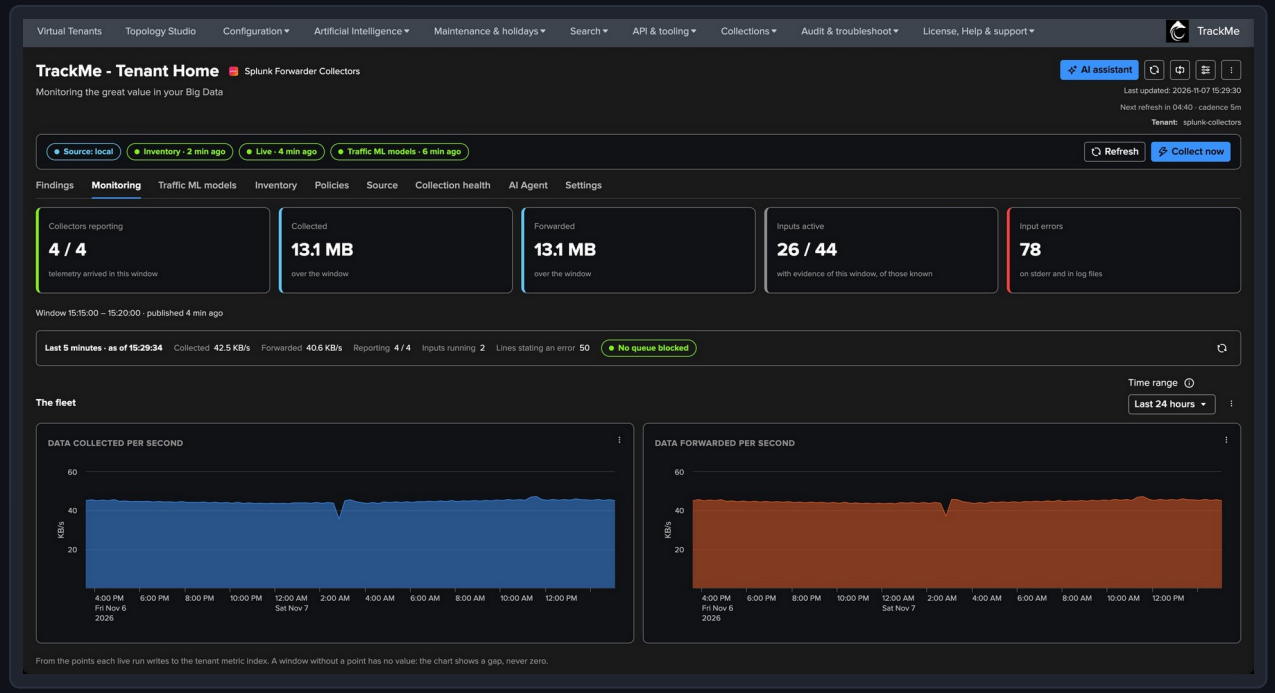
03

PART 3 · FOLLOW

Every collector, every input

Monitoring: the collectors, their inputs and processes; one collector up close; the inventory and the policies.

The latest window, the last five minutes, the last 24 hours



1 **Tiles**

Collectors reporting, collected, forwarded, inputs active, input errors.

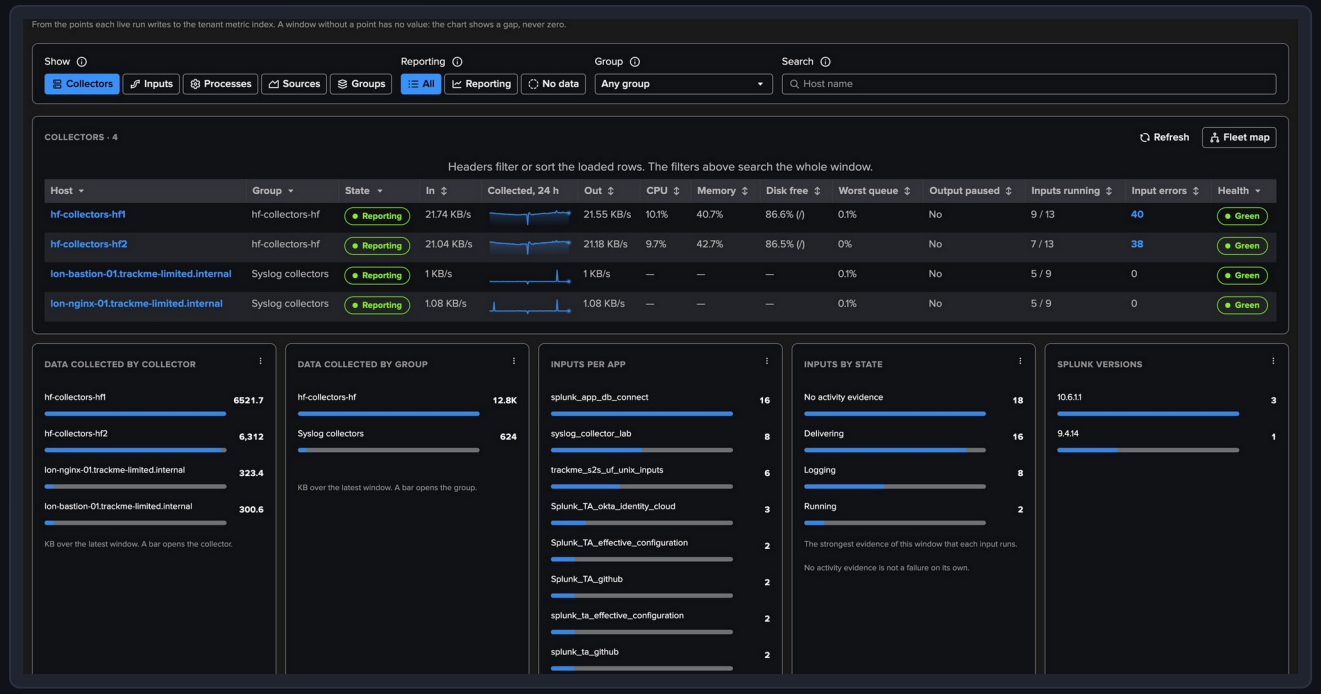
2 **Last 5 minutes**

Read on demand, with the queues blocked.

3 **The fleet**

Data collected and forwarded per second, over 24 hours.

The collectors — host, pipeline, inputs, health



1 In and out

What each collects and forwards, and 24 hours of it.

2 Host

CPU, memory, disk free: heavy forwarders only.

3 Pipeline

Worst queue, output paused.

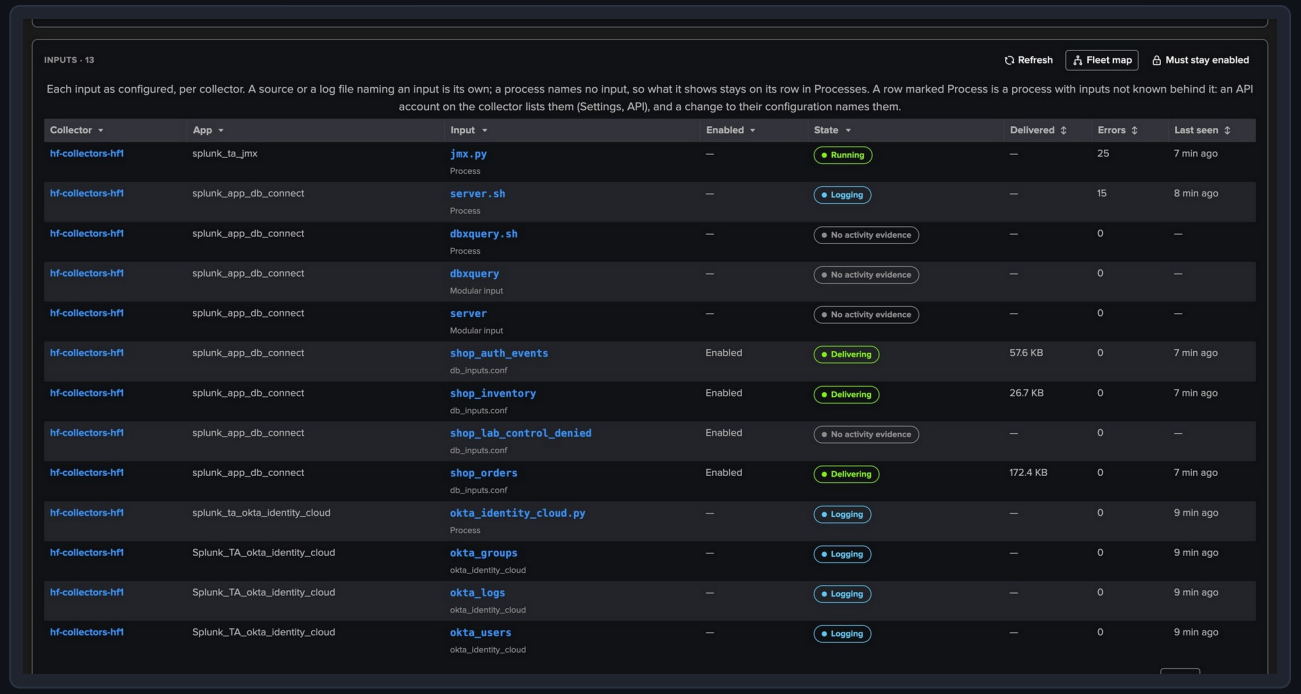
4 Inputs

Running of those known, input errors.

5 Breakdowns

By collector, group, app, input state, Splunk version.

Every input as configured — for any add-on



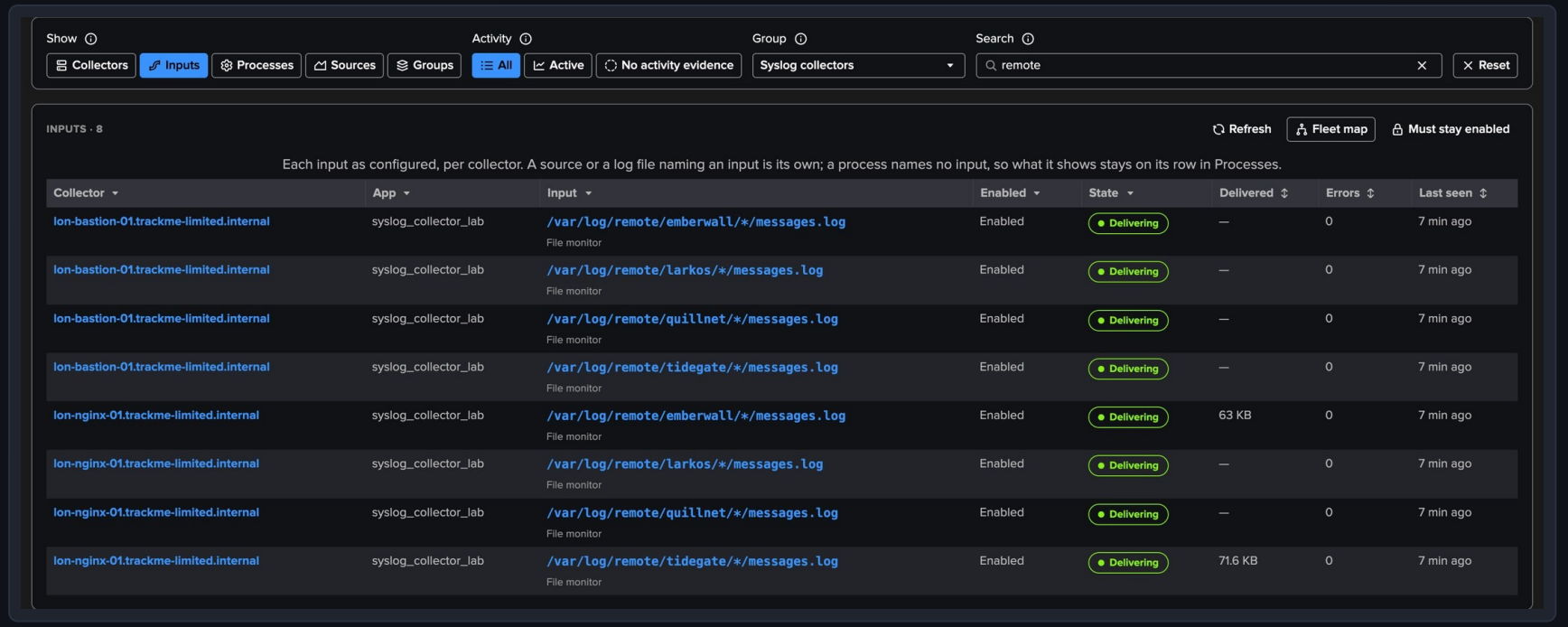
1. **JMX**
   A process with its errors on stderr: Running.

2. **DB Connect**
   Its inputs in db_inputs.conf, each Delivering its own source.

3. **Okta**
   One script, three stanzas, each Logging in its own file.

4. **No activity evidence**
   The modular input defaults: never a failure on its own.

Each monitor stanza of a syslog collector is an input



1 **Four vendor feeds**

On both forwarders, from /var/log/remote.

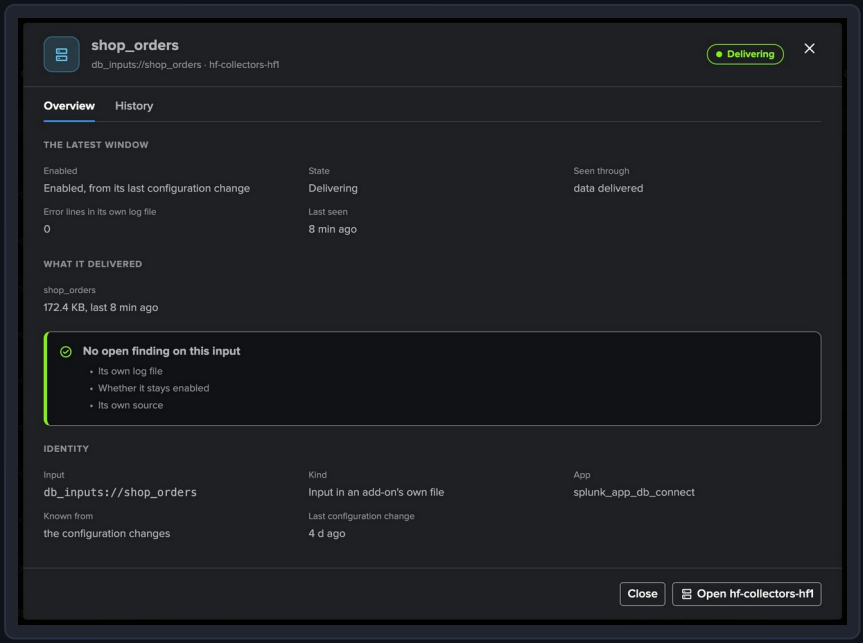
2 **Delivering**

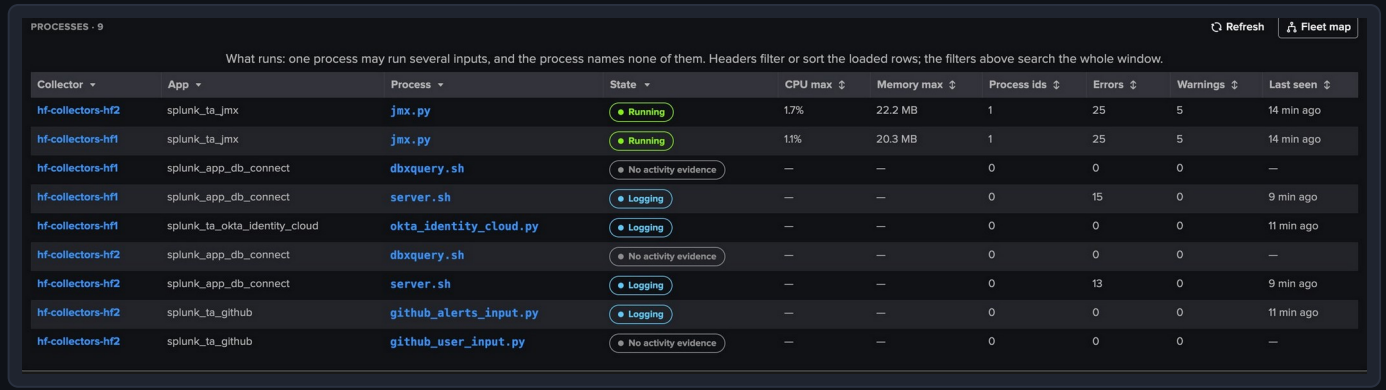
From what reached the indexes, judged once per group.

3 **Delivered**

Only where the forwarder's own metrics name the file.

An input up close — and the processes that run them





1 **The latest window**

Enabled, Delivering, seen through data delivered.

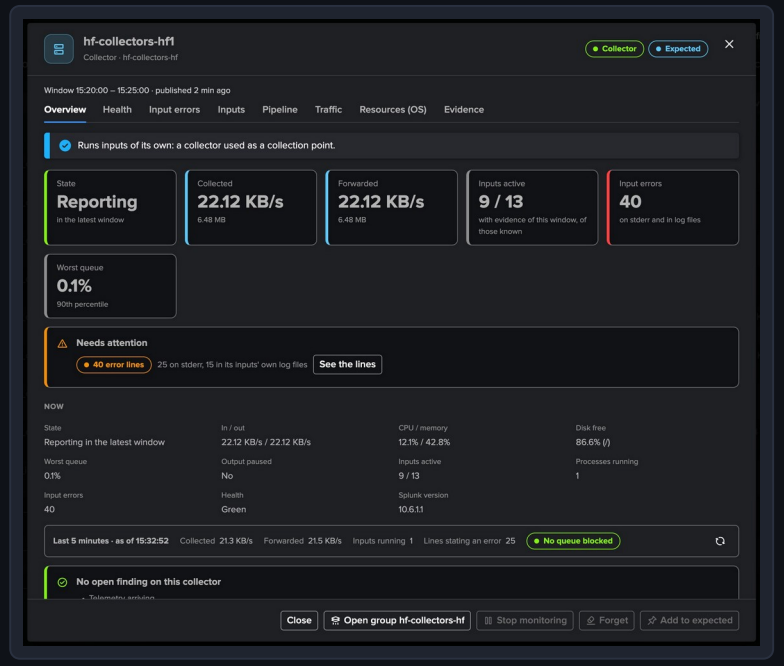
2 **Identity**

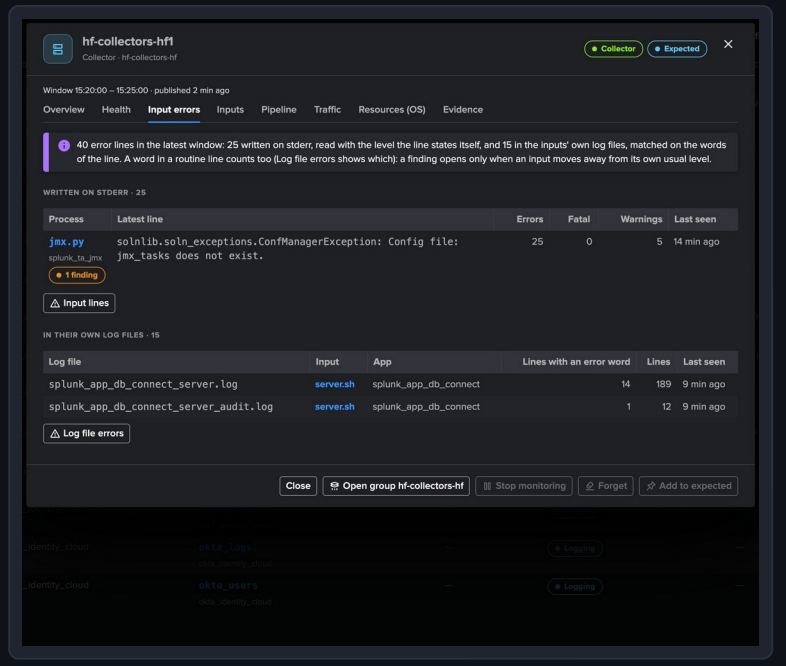
db_inputs://shop_orders, known from the configuration changes.

3 **Processes**

What runs, with its CPU, memory, process ids, errors and warnings.

One collector up close — what is wrong, first





1 Needs attention

40 error lines: 25 on stderr, 15 in its inputs' own log files.

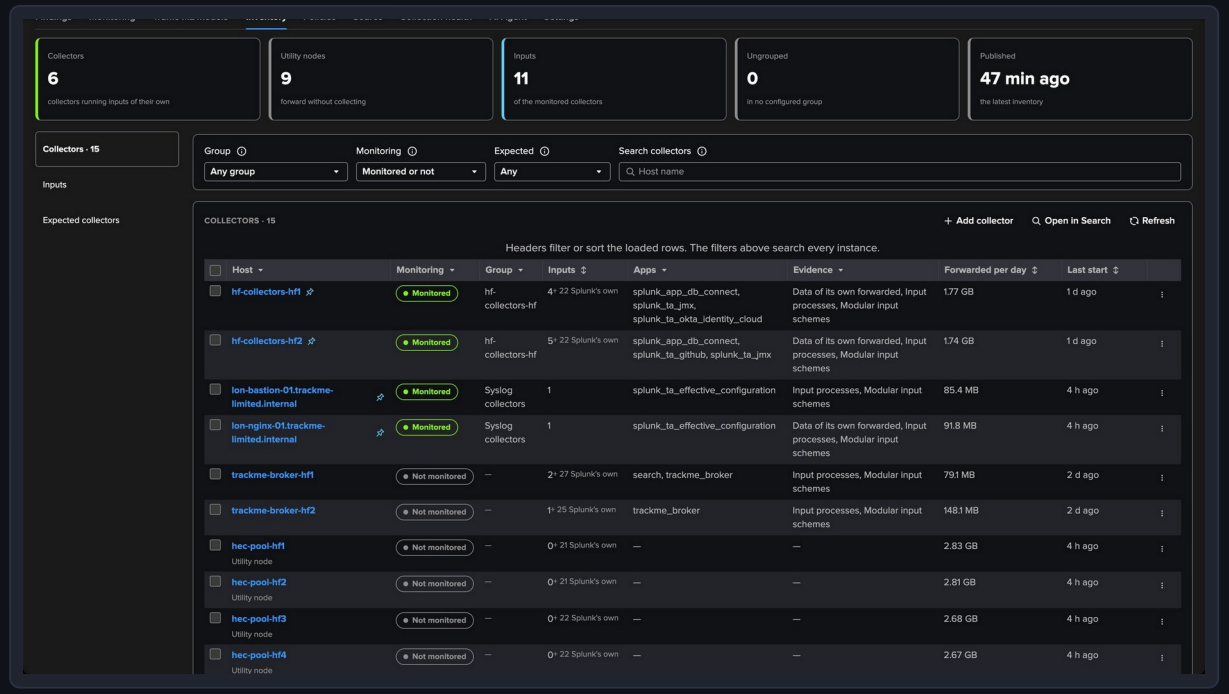
2 Input errors

Every error line by where it was written, adding up to the count.

3 Its own usual level

A finding opens only when an input moves away from it.

The inventory — what is monitored, and what is not



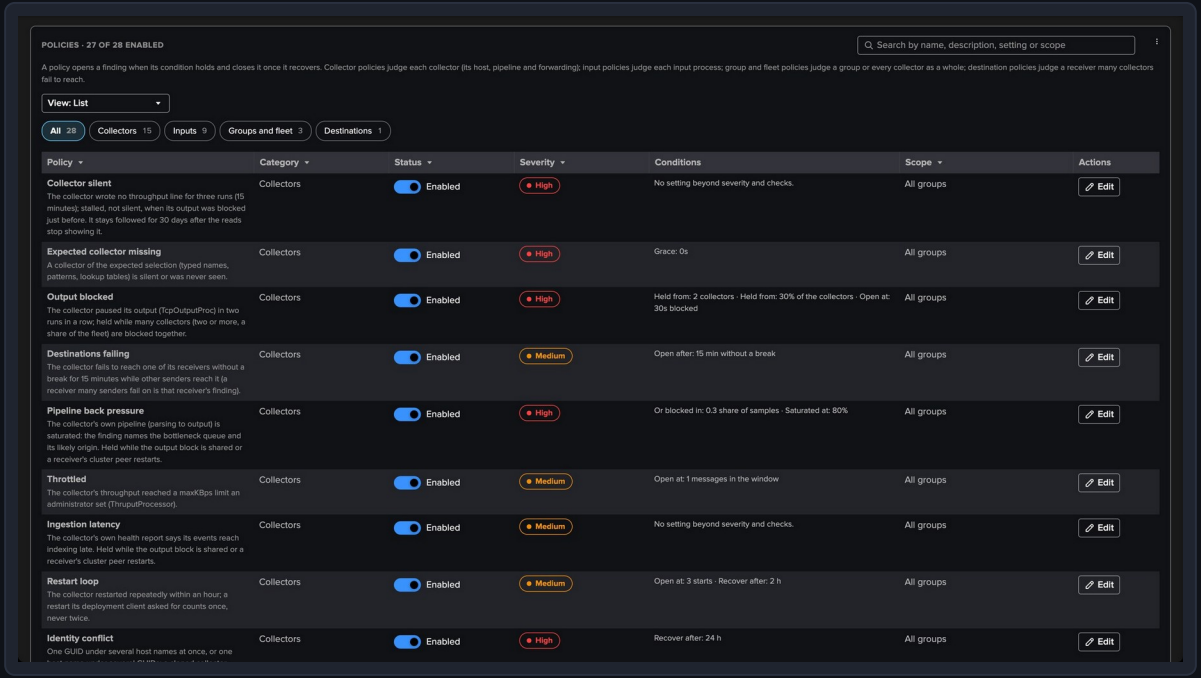
1. **Collectors and utility nodes**
   Every instance the inventory published.

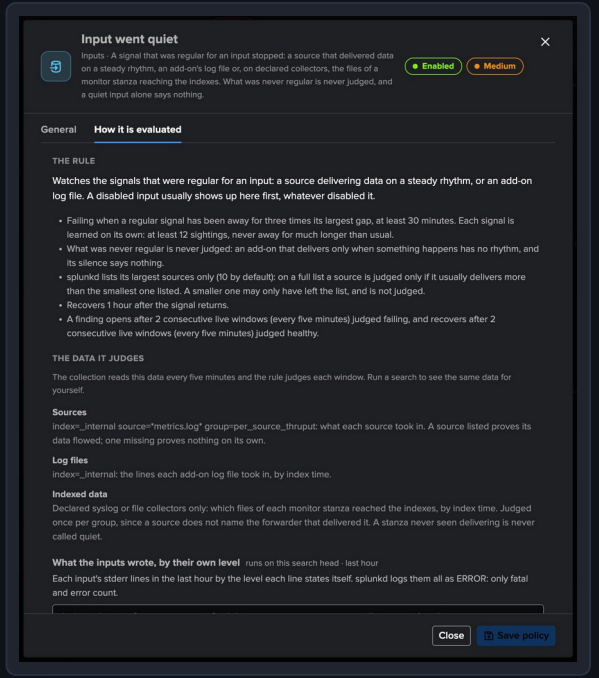
2. **Monitoring**
   Monitored or Not monitored: whether TrackMe follows it, never whether it runs.

3. **Stop and Resume**
   From the pill: out of Monitoring and its totals at once.

4. **Expected collectors**
   A pin; their silence is a finding at once.

Twenty-eight policies — and how each is evaluated





1 Collectors

Silent, expected missing, output, pipeline, restarts, identity, resources, disk, volume.

2 Inputs

Not running, errors, went quiet, process stopped, crash loop, file inputs.

3 Groups and fleet

Below minimum, version drift, mass silence.

4 How it is evaluated

The rule, the data with ready-to-run searches, how to resolve.

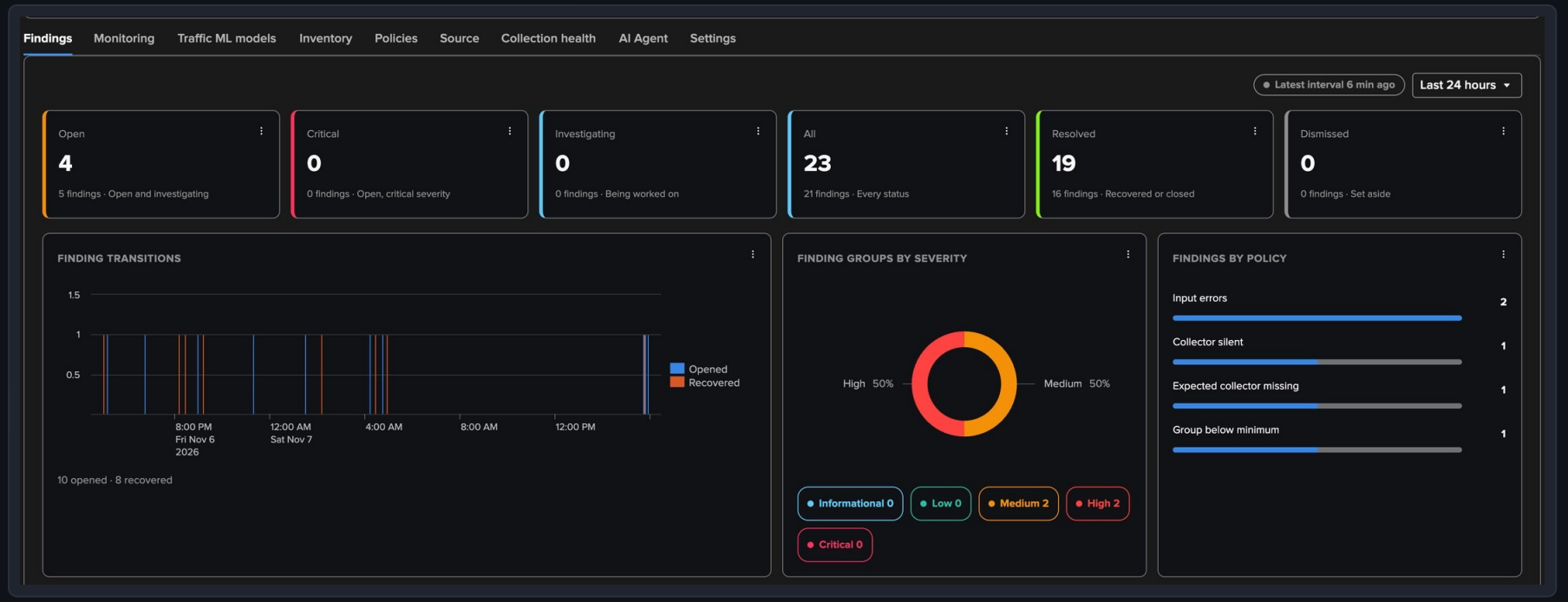
04

PART 4 · FINDINGS

An outage caused on purpose

A syslog collector stopped: what opens, and how it groups.

The findings — one per problem, grouped by object



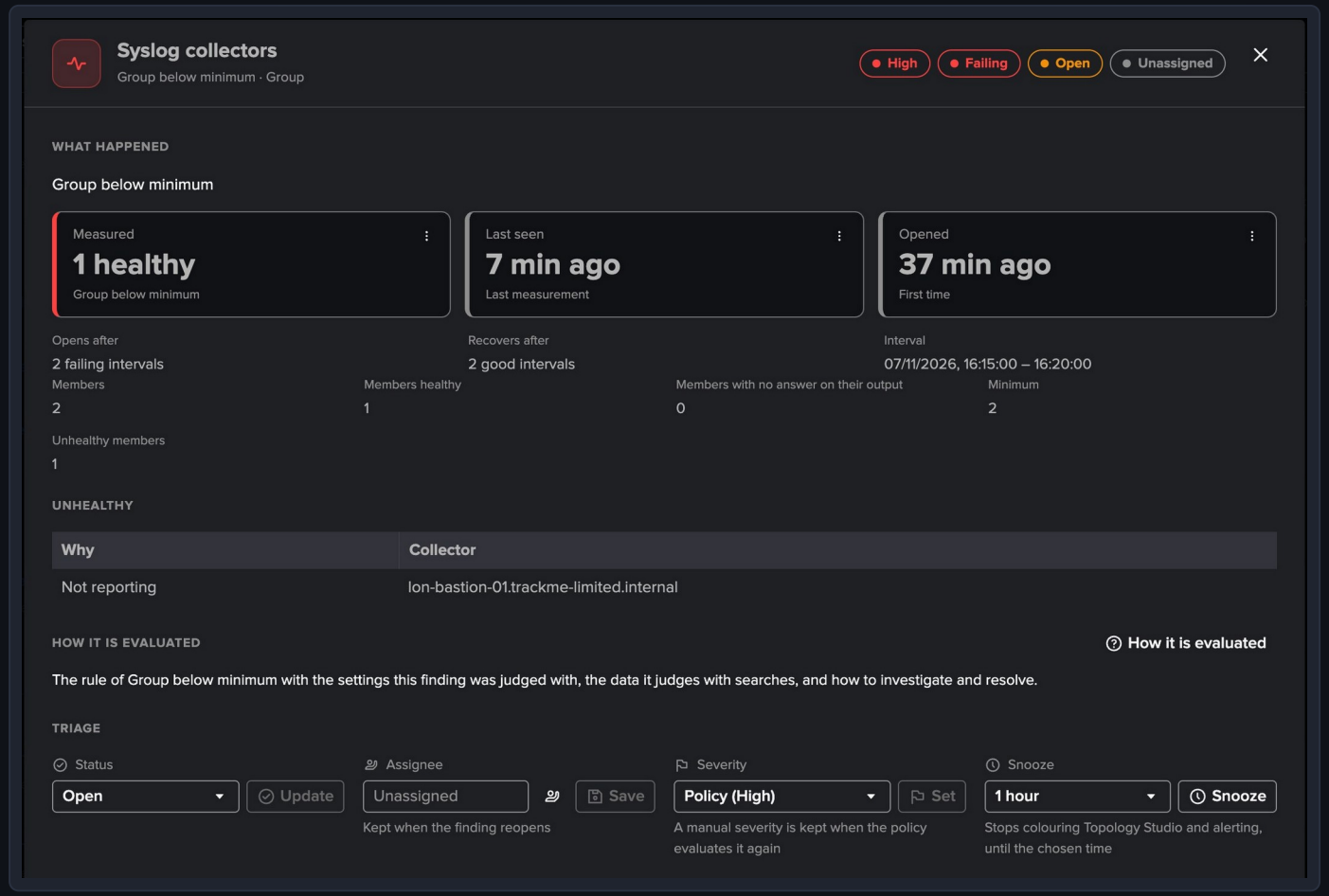
1 **Group below minimum**
Syslog collectors: one healthy member of a minimum of two.

2 **Collector silent**
The stopped forwarder, an expected collector too.

3 **Input errors**
The JMX add-on input, on both add-on collectors.

4 **By policy**
What opened, over the last 24 hours.

A group below its minimum — fewer healthy than you require

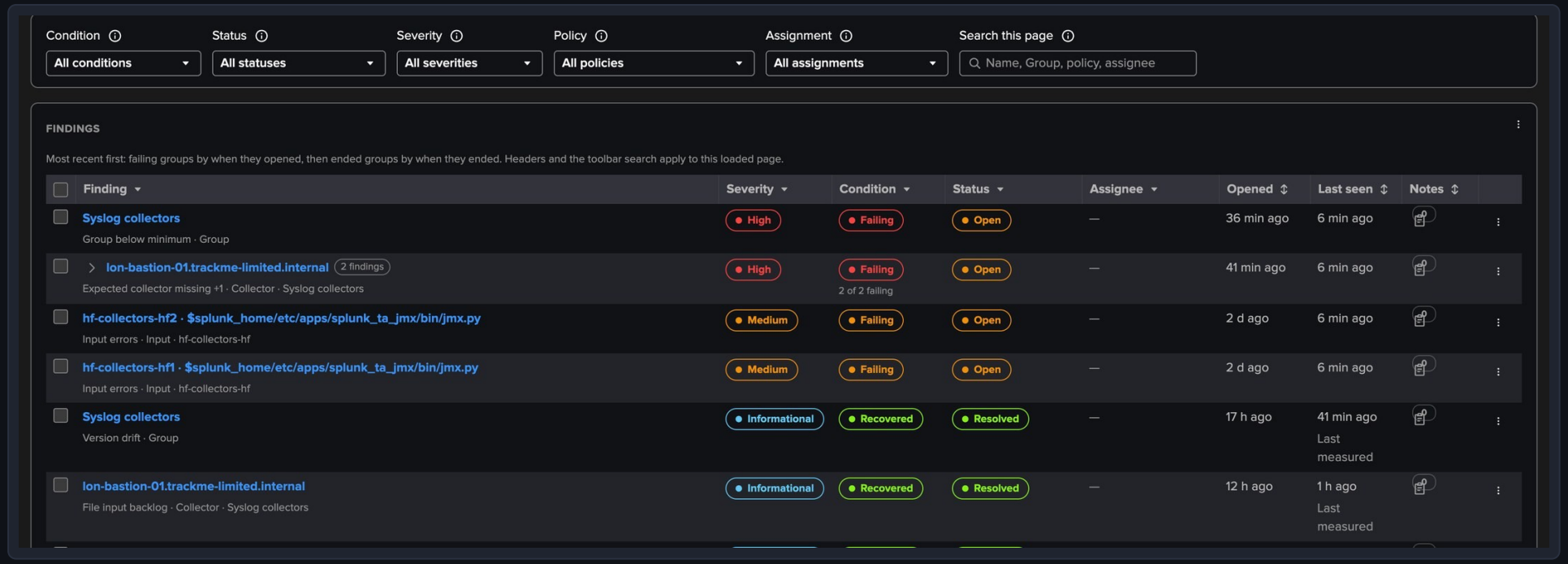


1. **Measured**
   One member healthy, against a minimum of two.

2. **Why**
   The unhealthy member and its reason: not reporting.

3. **Nothing learned**
   The minimum is yours; the health report does not count.

One Finding group per object — triaged once



1 The group

Group below minimum, high, on Syslog collectors.

2 The collector

Collector silent and Expected collector missing: 2 of 2 failing.

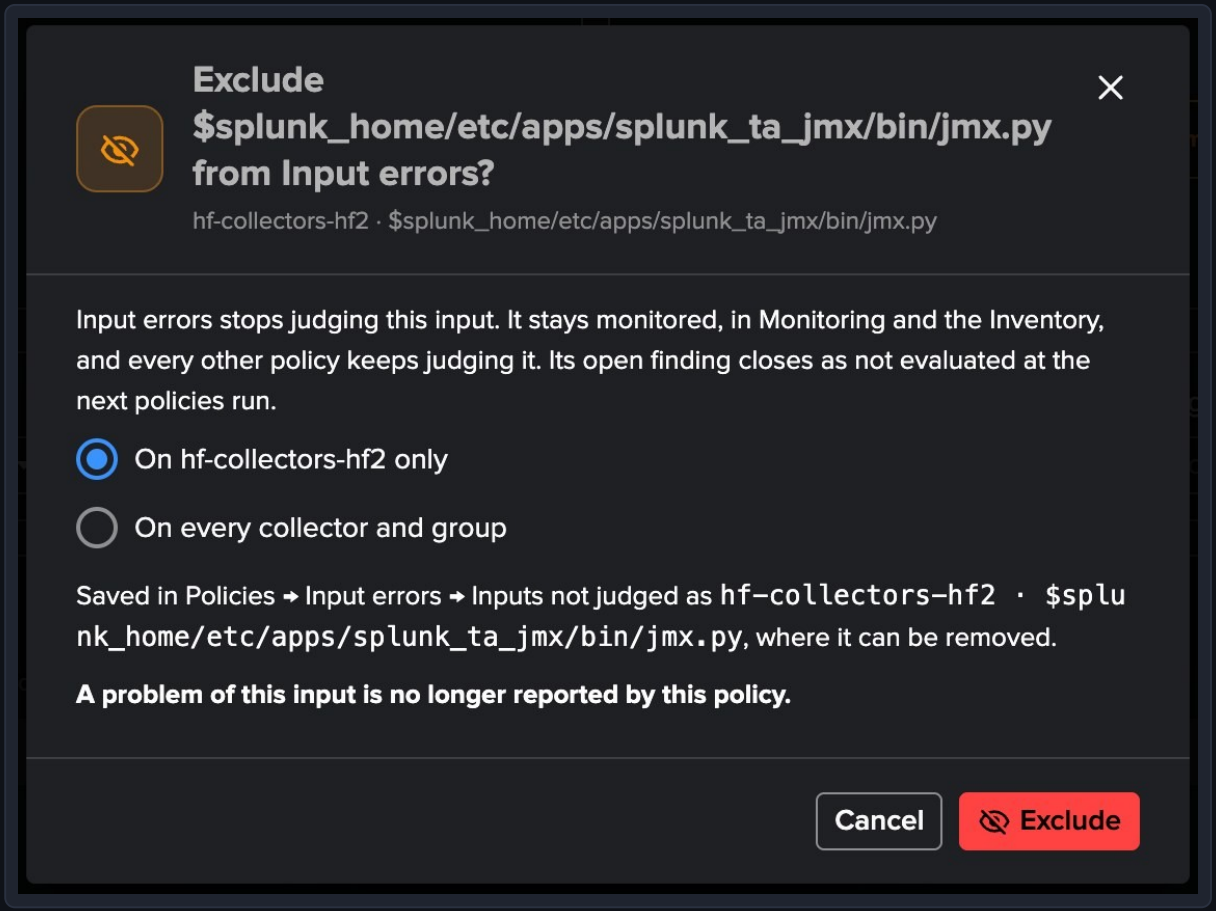
3 The input

JMX input errors, one finding per collector.

4 Recovered

Back by itself after the good intervals.

A false positive on one input — exclude it from one policy

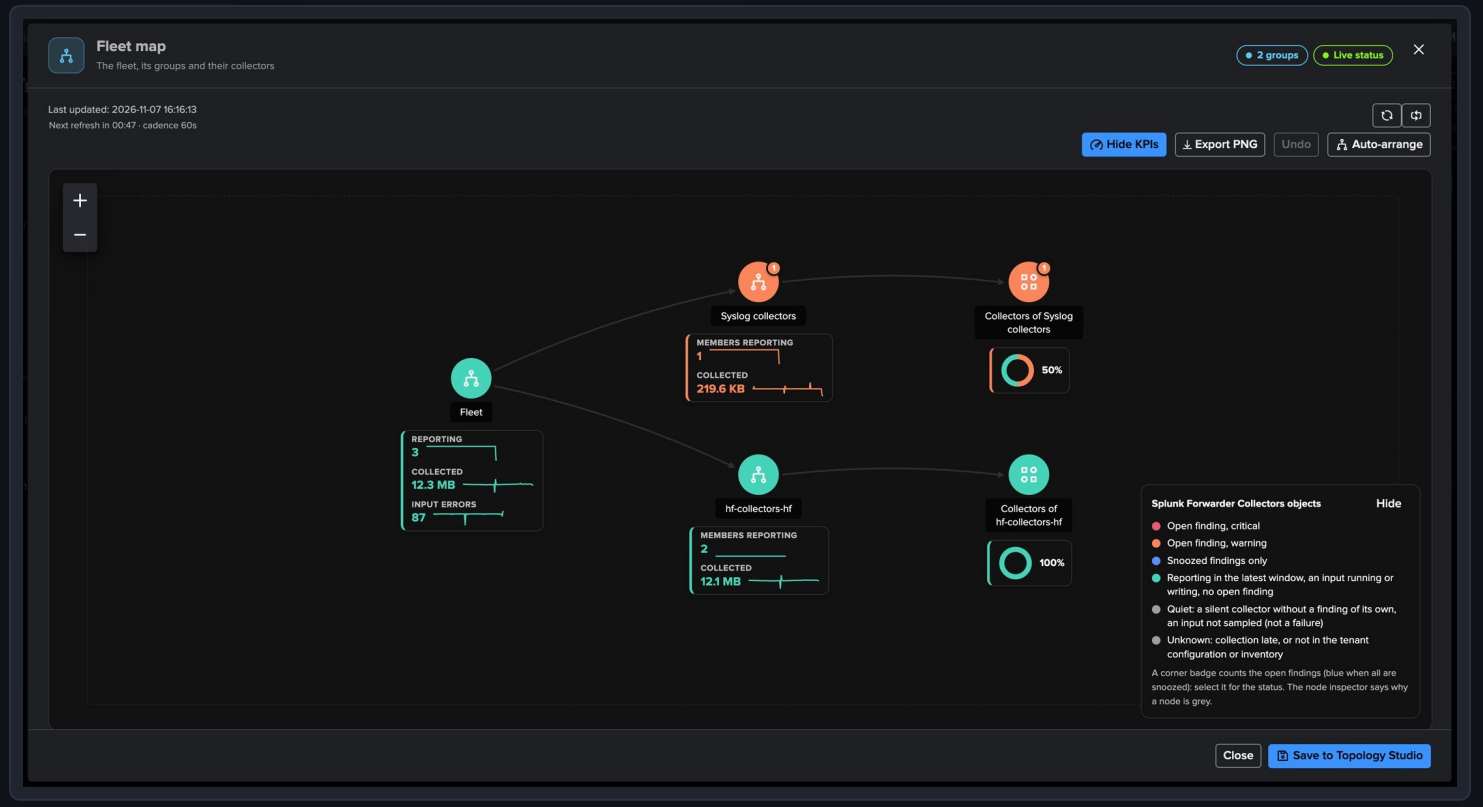


1. **One input, one policy**
   This collector only, or every collector and group.

2. **Still monitored**
   Every other policy keeps judging it; it keeps learning.

3. **Closed as not evaluated**
   Its finding closes at the next run; Include again undoes it.

The Fleet map — the fleet, its groups and their collectors



1. **Groups**
   Members reporting and what they collected, live.

2. **Status**
   From the open findings: the syslog group orange.

3. **Save to Topology Studio**
   Edit it as a view of your own.

WHERE WE ARE

One tenant, every collection point and every input

Set up

a tenant on the local search tier, two collector API accounts, the discovery

Configured

groups and a minimum, syslog collectors declared, inputs that must stay enabled

Followed

collectors, inputs and processes, a collector up close, the inventory

Judged

a group below its minimum, a silent collector, input errors

What made it work

Inputs, not processes

Every input as configured, judged by what it delivers and writes.

Declared, never guessed

A syslog collector is what you say it is.

Nothing to install

Splunk's own telemetry, no new data, remote accounts optional.