



HANDS-ON WALKTHROUGH · TOPOLOGY STUDIO

Your environment, as a live map

Maps built from real TrackMe entities that colour themselves with live health — generated from a tenant in a few clicks, authored by hand, alerting on the service they draw, or built from a sentence with AI.

Captured live on TrackMe 2.4.18 · Splunk Enterprise



Entities tell you what is broken. A map tells you what it breaks.

Operators think in services, sites and pipelines. An entity table, however well classified, is a list — and a diagram in a wiki is out of date the day after it is drawn.

The service is invisible

A red feed, three hosts behind it and a search that depends on it: the table shows four rows, not one broken service.

Diagrams go stale

Hand-drawn maps describe last quarter. New feeds are missing, retired ones are still drawn, and nobody trusts the colours.

Owners want one signal

A service owner wants to know when the service degrades — not one alert per entity, and not a colour they have to interpret.

What Topology Studio does

Topology Studio is a canvas for YOUR view of the environment: a payment flow, a data centre, an ingestion pipeline, a business service. Every node is a real TrackMe entity from any tenant and any component, a live aggregate of many entities, or another saved view. The map colours itself with live health, is shared under RBAC, and can alert on the service it draws.

Available in every edition — Foundation, Enterprise, Unlimited and trials — including authoring and Topology Alerts.

A view, its nodes, its links — and live health on every one

Entity

One monitored entity — any tenant, any of the seven components — with its live colour and up to five KPIs.

Scoped aggregate

Tenants × components + an optional filter. Worst member or healthy %. Dynamic membership; can draw its members.

Auto aggregate

A parent whose members are the nodes linked to it: a service built from existing blocks.

View node

Another saved view folded into one health node — a map of maps you can drill into.

Labels & decorations

Text, shapes and images to annotate zones, tiers and flows. No health of their own.

● Live

every node polls on a 60-second cadence, with a countdown, manual refresh and pause

● Honest

incomplete data reads unavailable, deleted entities read missing — never green by default

● Shared

a view has Can view / Can edit role lists; tenant masking is enforced per node on the server

● Versioned

every save is a version with non-destructive restore; views export and import between instances

Four ways to a map — one live view in the end

Part 1 • Generate

- From Tenant Home, one click: a live map of the tenant
- Hierarchy presets or a custom sequence of fields
- A condition such as high and critical only
- Save it as a view

Part 2 • Author

- An empty canvas and a root aggregate
- Two child aggregates from priority and labels
- Members drawn automatically, with KPIs and sparklines
- Links, auto-arrange, save

Part 3 • Alert

- A Topology Alert on the view
- Transitions only: open, update, resolve
- The rendered map in the email
- Run history and events

Part 4 • AI

- Build with AI from one sentence
- A live preview with health
- Refine the draft in plain words
- Create the view

Then a few maps that run in production: a Cribl pipeline, a public web estate, and a map of maps over the Splunk infrastructure.

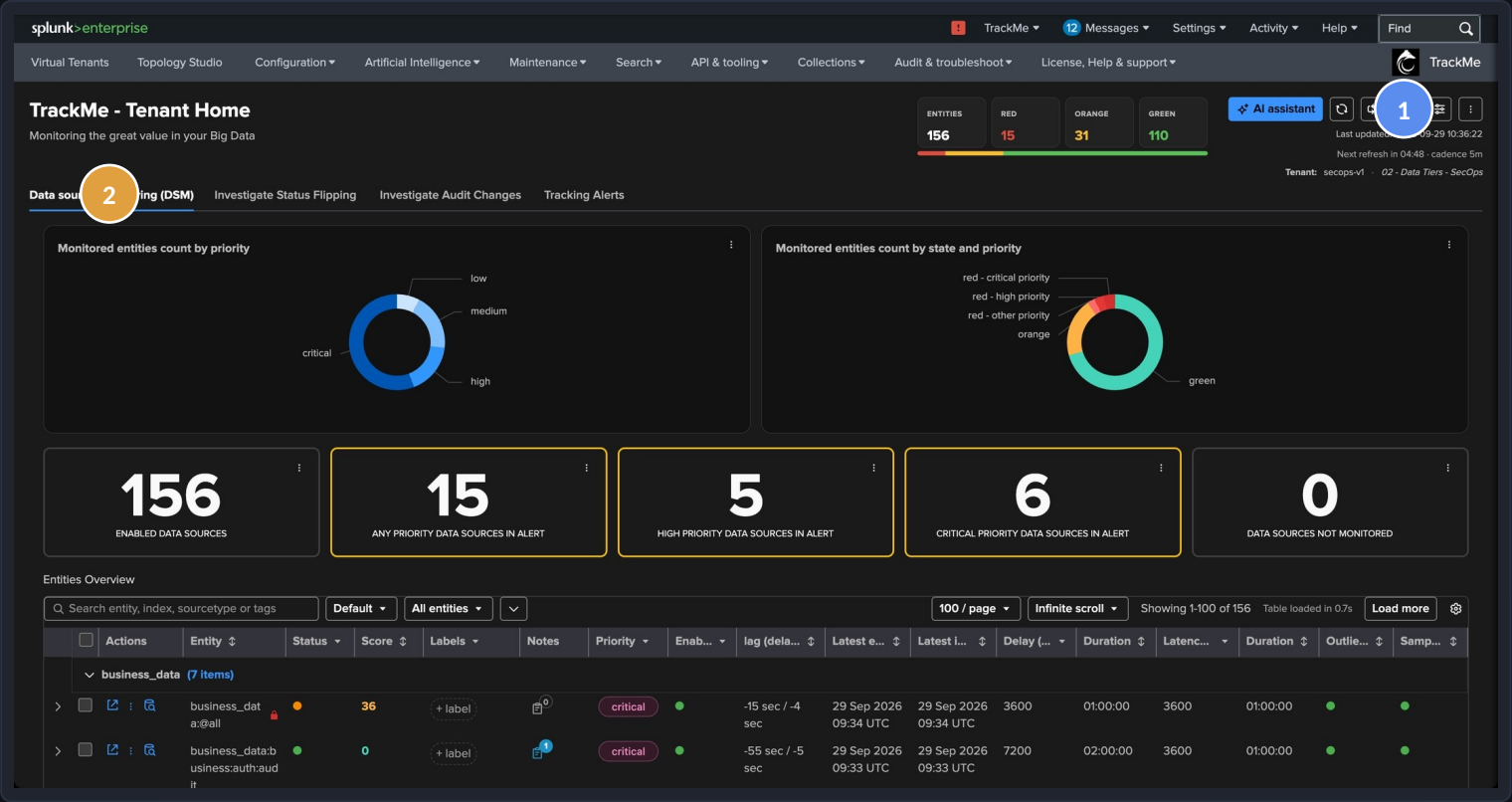
01

PART 1 • GENERATE

A live map of a tenant, in a few clicks

Tenant Home turns any tenant into a structured topology: a root aggregate, one live aggregate per group, any hierarchy you like — then save it as a view.

Tenant Home — the topology icon



1 **Open the tenant topology**
The icon at the top right of Tenant Home generates a topology of the component you are looking at.

2 **The component in view**
Here the data sources (DSM) of a SecOps tenant. The same works for DHM, MHM, FLX, WLK, FQM and VOL.

Nothing to prepare

No view to create, no node to place: the tenant already carries the structure — indexes, tags, priorities, labels. The generated map is temporary until you save it.

The default map — one aggregate per index



- 1 **Temporary topology**
Nothing is saved yet; the banner says how many entities are represented.
- 2 **Hierarchy**
Default for DSM is per index — change it with one selector.
- 3 **Include entities · Entity limit**
Aggregates only by default; entity nodes on demand, within a limit.
- 4 **Condition**
An optional filter applied to every generated aggregate.
- 5 **Root aggregate**
The tenant itself, with its live healthy percentage.
- 6 **Save as topology view**
Freezes membership and layout; health stays live.

Hierarchy — presets, or your own sequence of fields

ore before saving.

Hierarchy: Default (Index) ▾

Include entities Entity limit 150 Save as topology view

ty IN ("high", "critic

Hierarchy: Default (Index) ✓ 1

Apply Last updated: 2026-09-29 10:36:42

ts. Apply rebuilds; clear and apply to

Hierarchy: Tenant only

Hierarchy: Index

Hierarchy: State

Hierarchy: Priority

Hierarchy: Sourcetype

Hierarchy: Tags 2

Hierarchy: Labels

Hierarchy: Anomaly reason

Hierarchy: Custom... 3

Hide KPIs Export PNG Undo Auto-arrange

Next refresh in 00:42 · cadence 60s

m-infra-apac siem-osnix-amer siem-osnix-latam siem-syslog-emea siem-vuln-apac siem-web-amer siem-web-latam

HEALTHY % HEALTHY 75% HEALTHY 75% HEALTHY 100% HEALTHY 75% HEALTHY 83% HEALTHY 60%

siem-wineventlog-emea

1 Presets

Default, tenant only, index, state, priority, sourcetype, tags, labels, anomaly reason — the groupings of Tenant Home.

2 Tags

One aggregate per tag value — the ownership view as a map.

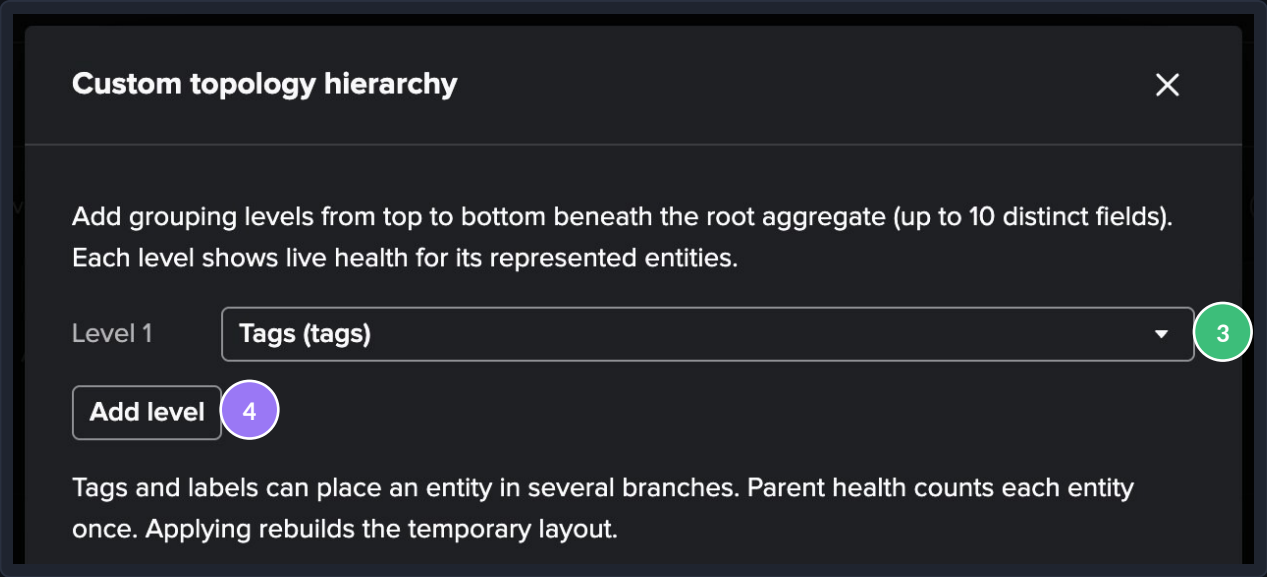
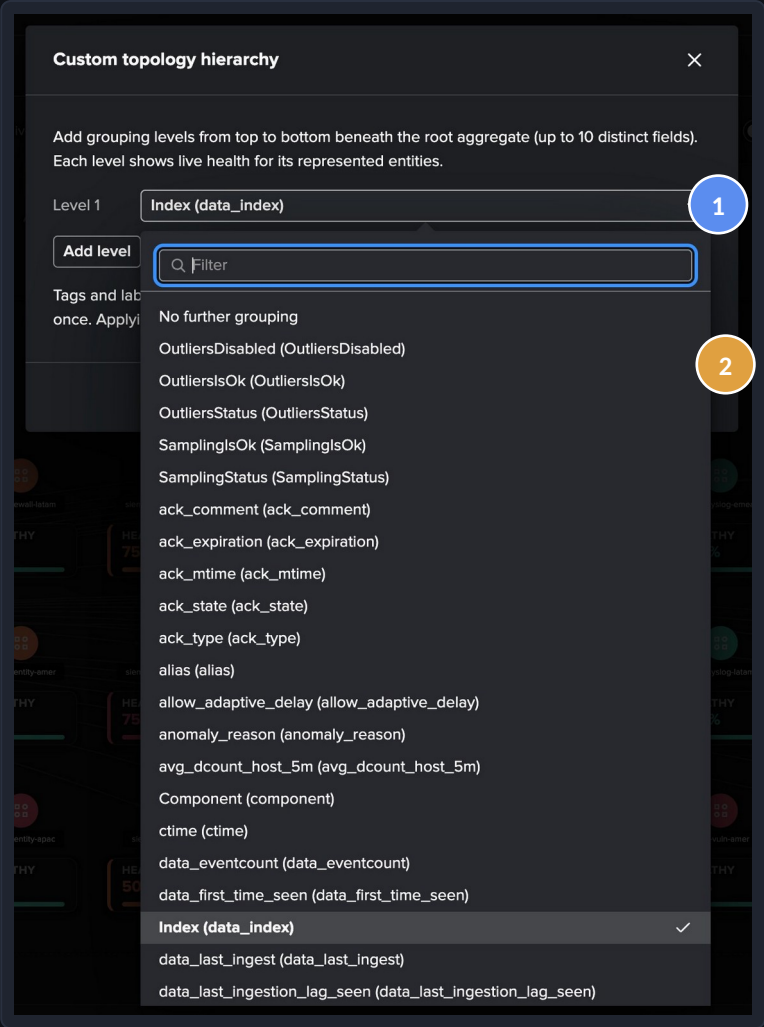
3 Custom...

Any sequence of entity fields, from top to bottom beneath the root.

Per component

FLX offers group and subgroup, WLK overgroup and subgroup, FQM datamodel, VOL licence pool and detection direction — the presets follow the component.

Custom hierarchy — any entity field, level by level



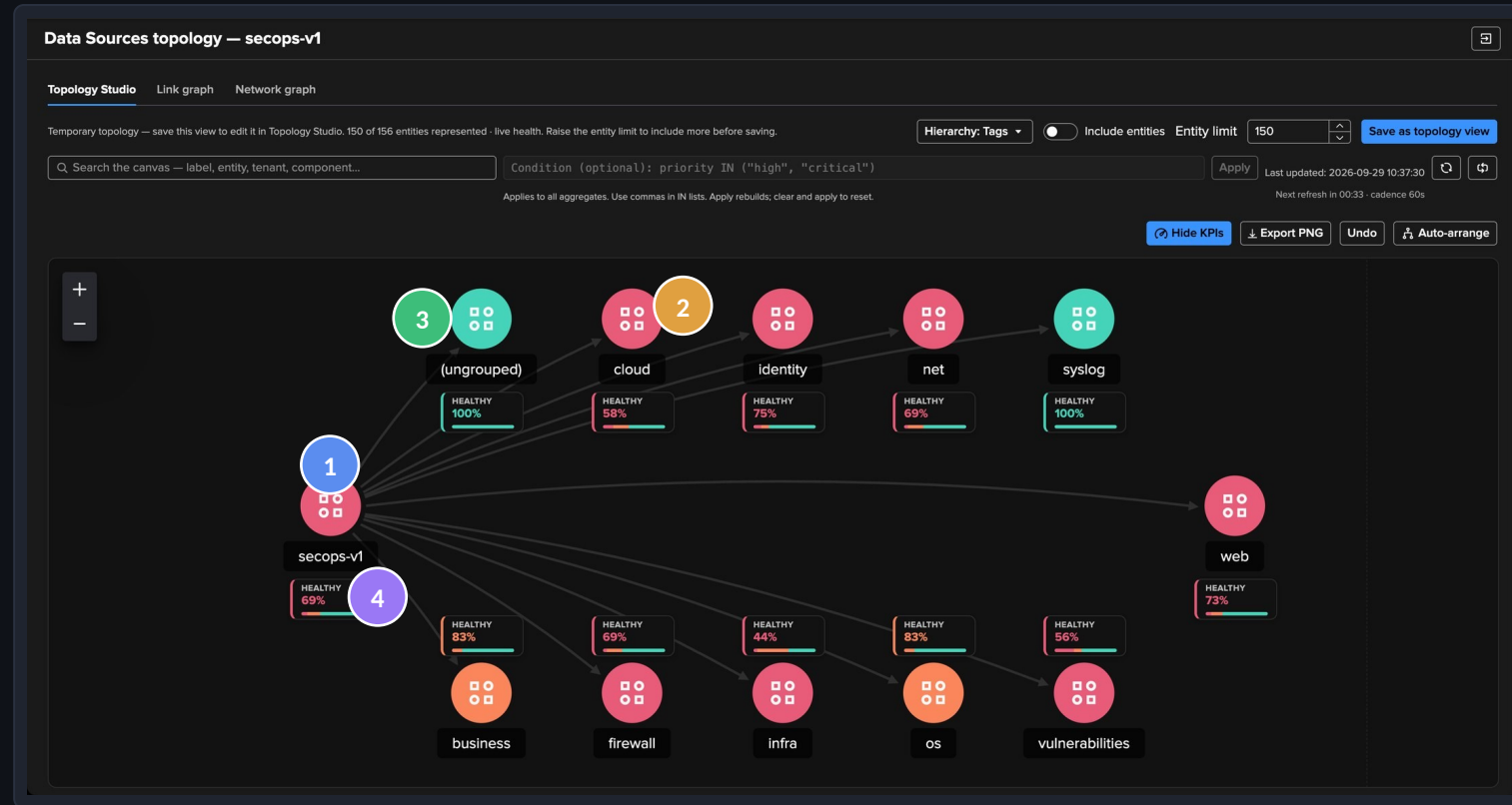
1 **Level 1**
Each level picks one field of the entity records.

2 **Every field**
Tags, labels, priority, state, index, sourcetype — and the component's own fields.

3 **Tags as level 1**
An entity with several tags appears under each of them; parent health counts it once.

4 **Add level**
Up to ten levels — for example Tags, then Priority beneath.

Grouped by tag — the ownership view, as a map



1 The tenant

The root aggregate over every monitored entity of the tenant.

2 One aggregate per tag

cloud, firewall, identity, net, web... each a live aggregate with its own colour.

3 (ungrouped)

Entities without a tag are not lost: they are grouped explicitly.

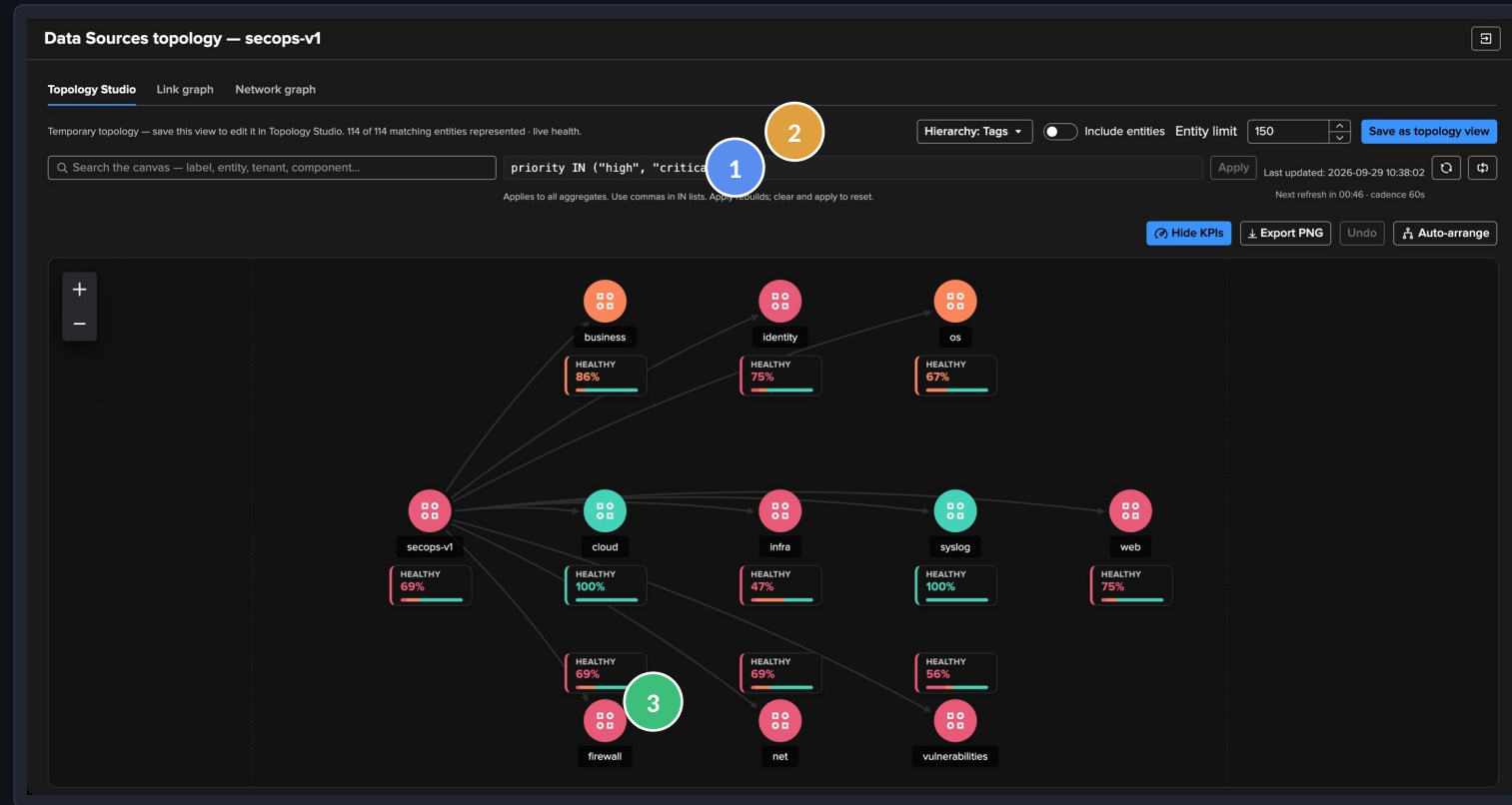
4 Healthy percentage

The KPI of each aggregate — hide or show KPIs from the toolbar.

Auto-arrange

Direction, spacing and canvas size in one popover; the arrangement is a single undo step.

A condition — high and critical only, and the map is ready



1 priority IN ("high", "critical")

The filter syntax of Virtual Groups, applied to every aggregate including the root.

2 Matching entities

The banner counts the entities the condition keeps.

3 What matters, by owner

The low-priority noise is gone; (ungrouped) disappears with it.

The same syntax everywhere

field=value with wildcards, AND / OR, parentheses, IN lists — the language of Virtual Groups, ML scopes and aggregate filters.

Save as topology view — a map anyone can open

Create topology view

View ID *

secops-v1-topology

Type freely — the identifier is derived automatically. Unique, cannot be changed later.

Display name *

secops-v1 topology

Description

Created from Tenant Home. Membership captures the selected entities; health refreshes live.

Category

Optional grouping label, e.g. Production

Pick an existing category or type a new one. Views sharing a category are grouped under one heading.

Can view (roles) *

trackme_admin × trackme_power × trackme_user ×

Read-only access. Admin roles always have access regardless of this list, and roles with edit access below can always view.

Can edit (roles) *

trackme_admin × trackme_power ×

Roles allowed to modify or delete this view. Admins and the view's creator always keep edit access; listed roles still need TrackMe power permissions, so user-tier roles remain read-only either way.

Cancel

Create view

1 View id and display name

The id is derived from what you type and cannot change later; the name can.

2 Category

Pick an existing one or type a new one; the views browser groups by category.

3 Can view (roles)

Read access. Administrators always have access.

4 Can edit (roles)

Write access. The creator always keeps edit access.

What saving freezes

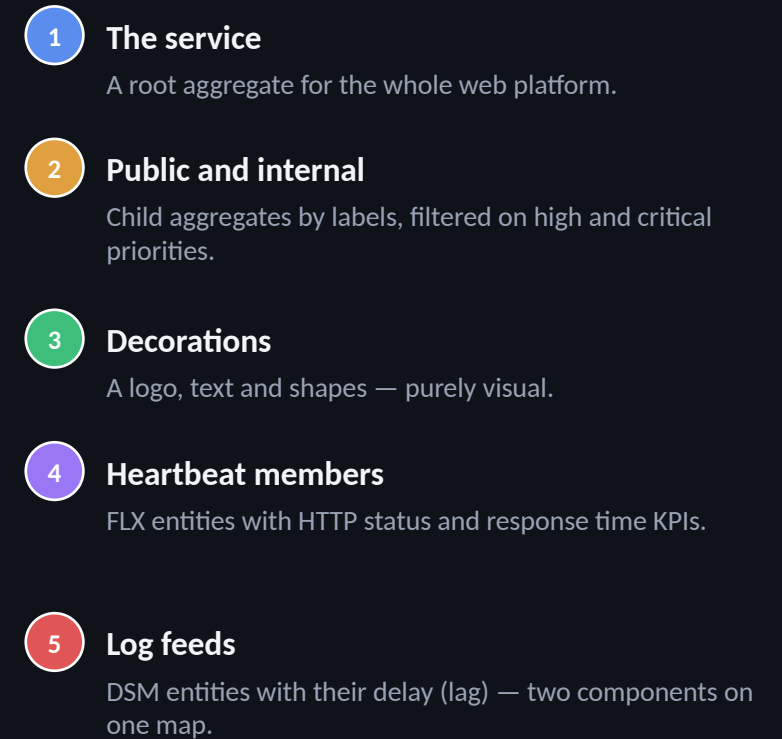
Membership and layout are frozen; health stays live. For membership that follows the tenant, author aggregates (Part 2) — they stay dynamic.

02

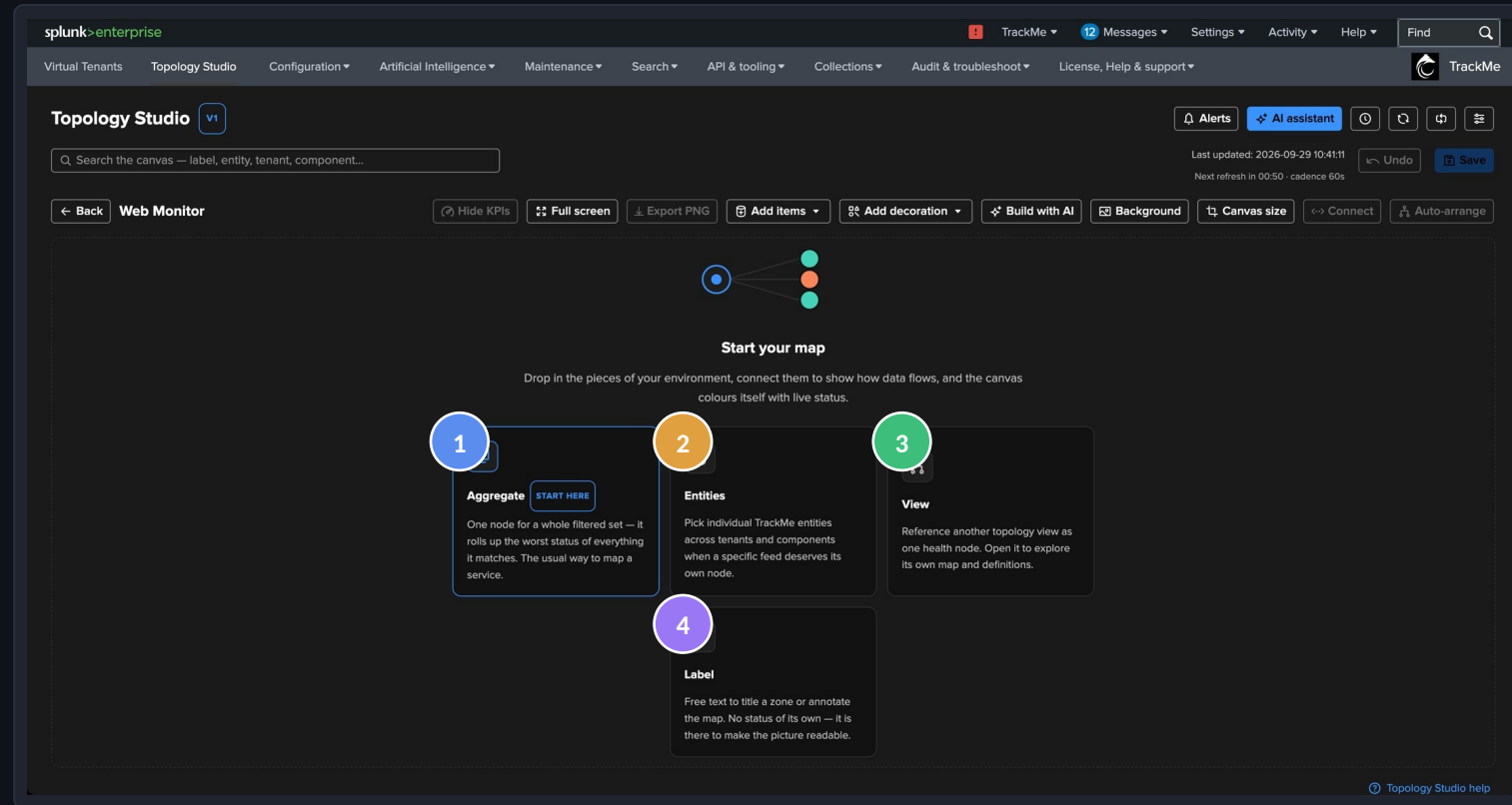
PART 2 · AUTHOR

From an empty canvas to a live service map

A root aggregate, two child aggregates from priority and labels, members drawn automatically with KPIs and sparklines — the way to map a service.



A new view — the canvas tells you where to start



1 Aggregate — start here

One node for a whole filtered set of entities: the usual way to map a service.

2 Entities

Individual entities when a specific feed deserves its own node.

3 View

Another saved view as one health node.

4 Label

Free text to title a zone or annotate the map.

Create topology view

Views browser → Create topology view: the same dialog as in Part 1 — id, name, description, category, roles. Here: Web Monitor, category Infrastructure.

The root aggregate — scope and filter

Add an aggregate node

An **aggregate node** rolls a whole group of entities up to one node: pick one or more tenants and their components, optionally narrow with a filter or an exact member selection, and choose whether the node's health follows its **worst member** or configurable **healthy-percentage thresholds**. With no exact selection, membership stays dynamic and newly discovered matches are covered automatically.

Node label *

Web Monitor

Scope * 3 of 8 tenant × component pairs

prod-trackme

Remove

DSM

DHM

FLX

+ Add tenant

Filter (optional)

Syntax: field=value — wildcards supported (* any sequence, ? one char). Space = implicit AND. Use OR for alternatives, parentheses for grouping, field IN ("a", "b") for lists. Case-insensitive.

priority IN ("high", "critical") AND labels IN ("public-facing", "internal-tooling")

Filter expression is valid.

Available fields

Select exact members (optional)

Health calculation

Cancel

Add aggregate

1 Node label

Web Monitor — the service this map is about.

2 Scope: tenant

Up to eight tenant × component pairs; add tenants for cross-tenant services.

3 Components

The tenant's enabled components are pre-ticked: DSM, DHM and FLX here.

4 Filter

priority IN ("high", "critical") AND labels IN ("public-facing", "internal-tooling") — validated as you type.

5 Exact members

Optional. Without it, membership stays dynamic.

TrackMe for Splunk · Hands-on: Topology Studio

docs.trackme-solutions.com

Preview before adding — the entities it will roll up

Add an aggregate node

Filter expression is valid.

Available fields

Select exact members (optional)

Health calculation

Worst member
1

Any red member makes the aggregate red; otherwise the worst member wins. This strict calculation does not use percentage thresholds.

Show KPI on canvas
2

Enables this aggregate's healthy-percentage KPI. Each viewer can still show or hide all enabled KPIs from the canvas toolbar.

Automatically show and link member entities
3

The matching entities render as linked nodes around this aggregate — membership stays live (newly discovered entities appear automatically, worst states first).

Preview

GREEN
16 entities matched
100% healthy
4

green: 16

Auto-generated entities (16)

webserver:apache:access:kvirawkey:url_domain|docs.trackme-solutions.com
GREEN
prod-trackme
DSM

webserver:apache:access:kvirawkey:url_domain|downloads.trackme-solutions.com
GREEN
prod-trackme
DSM

webserver:apache:access:kvirawkey:url_domain|licenses.trackme-solutions.com
GREEN
prod-trackme
DSM

webserver:apache:access:kvirawkey:url_domain|trackme-solutions.com
GREEN
prod-trackme
DSM

webserver.nginx:plus:kvkey:website|jenkins.trackme-limited.com
GREEN
prod-trackme
DSM

Cancel
Add aggregate

1 Health calculation

Worst member (any red member makes it red) or healthy percentage with two thresholds.

2 Show KPI on canvas

The healthy-percentage KPI under the node.

3 Show and link members

Draw the matching entities around the aggregate — kept off on the root.

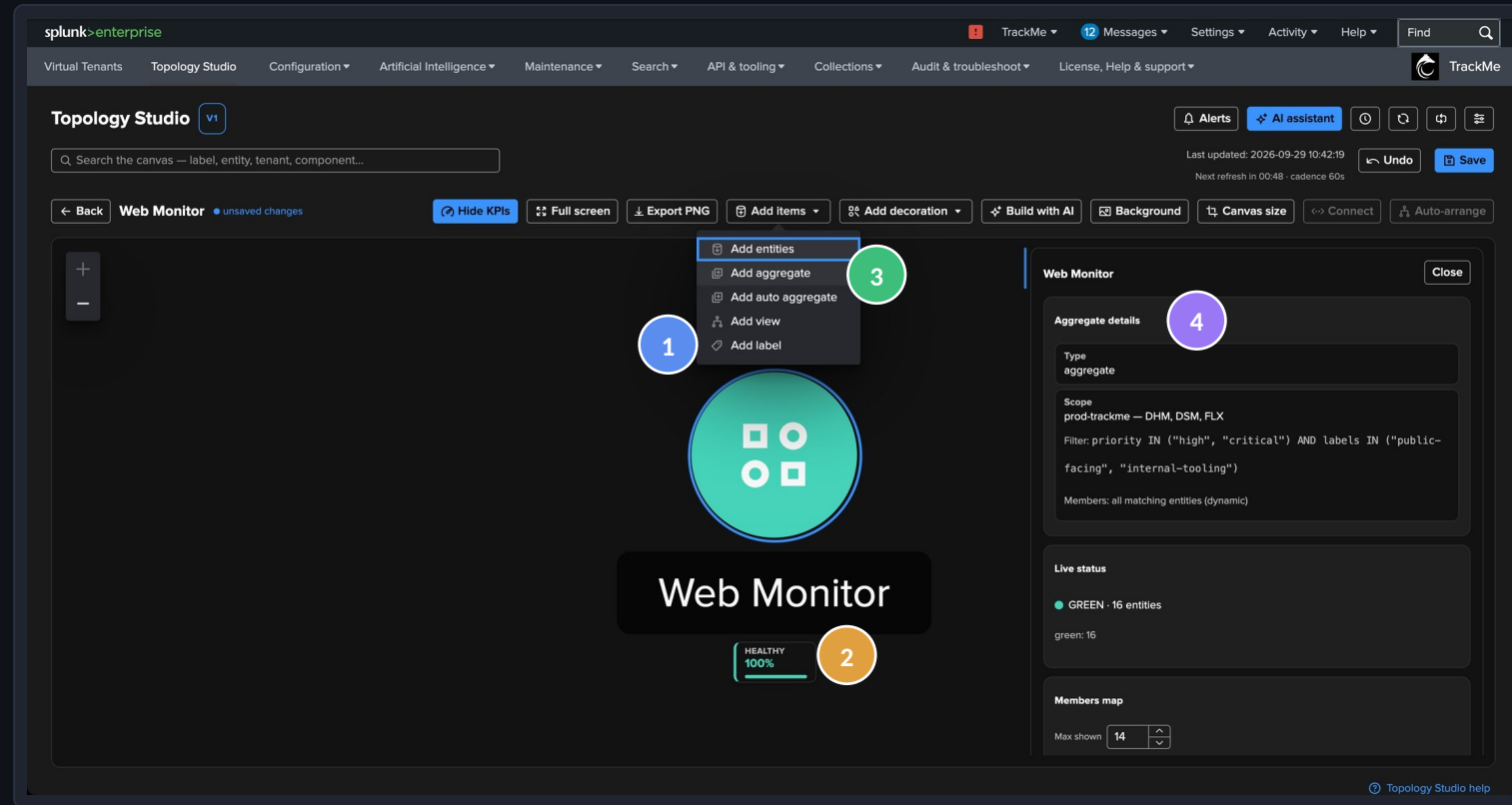
4 Preview

The live state and the count of matching entities.

5 The members

Every matching entity, with its state, tenant and component.

The root is on the canvas — now its two children



1 Web Monitor
The root aggregate, green, with its healthy percentage.

2 KPI
HEALTHY 100% — every member is green.

3 Add items
Entities, aggregate, auto aggregate, view, label.

4 Inspector
Aggregate details, live status and a members map for the selected node.

Two children

Public Facing Web — labels IN ("public-facing"); Internal Tooling Web — labels IN ("internal-tooling"). Same scope, same priority filter.

Members drawn automatically — with KPIs and sparklines

Add an aggregate node

Worst member

Any red member makes the aggregate red; otherwise the worst member wins. This strict calculation does not use percentage thresholds.

Show KPI on canvas

Enables this aggregate's healthy-percentage KPI. Each viewer can still show or hide all enabled KPIs from the canvas toolbar.

Automatically show and link member entities

The matching entities render as linked nodes around this aggregate — membership stays live (newly discovered entities appear automatically, worst states first).

Auto-generated entity options

Only show entities in alert

On each refresh, matching entities in red are added to the canvas and removed when they leave red. Pinned entities remain on the map.

Auto-entities filter (optional)

Syntax: field=value — wildcards supported (* any sequence, ? one char). Space = implicit AND. Use OR for alternatives, parentheses for grouping, field IN ("a", "b") for lists. Case-insensitive.

priority=high OR priority=critical
object=*example*

Empty = every entity in scope.

Available fields

Applied after the aggregate scope, filter, and exact selection. It only controls which generated entities appear on the canvas; aggregate health and counts stay unchanged.

Max entities shown

30

Cancel

Add aggregate

Artificial Intelligence

Add an aggregate node

Max entities shown

30

Beyond this, the node shows "+N more".

Default icon

Default (by type)

Applied to every generated entity. A per-entity icon override still wins.

Show "auto" on generated links

Shows the non-removable "auto" marker on these links in the editor.

Entity label field

Alias

Labels the auto-generated entities with this field. Alias is always available (it defaults to ...)

Stat card

Label and value in a compact card

Coloured value

Card-free label and state-coloured value

Status badge

Label and value in a compact coloured pill

Sparkline

Label, value and a 24h mini trend line

Stat card

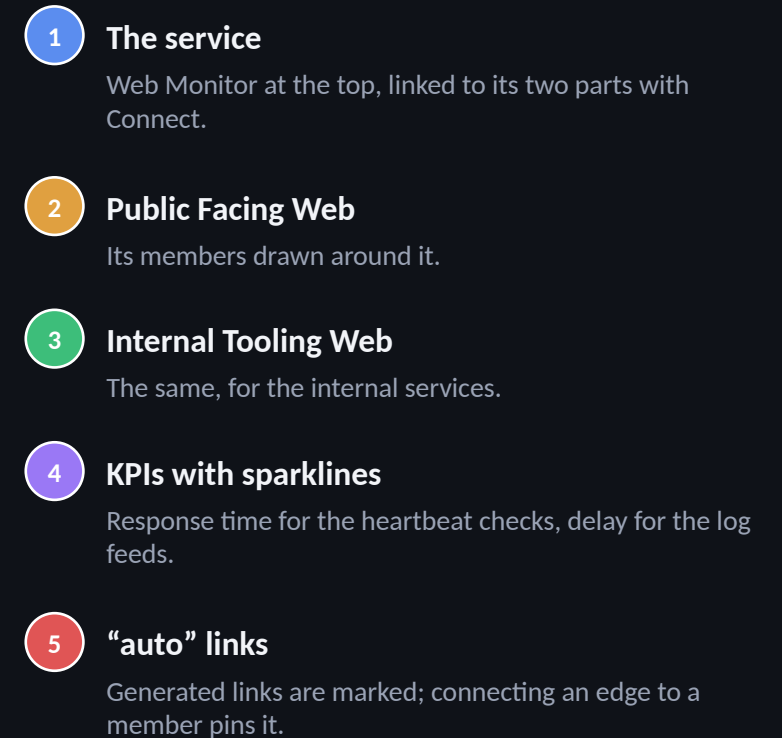
Label and value in a compact card

Preview

Cancel

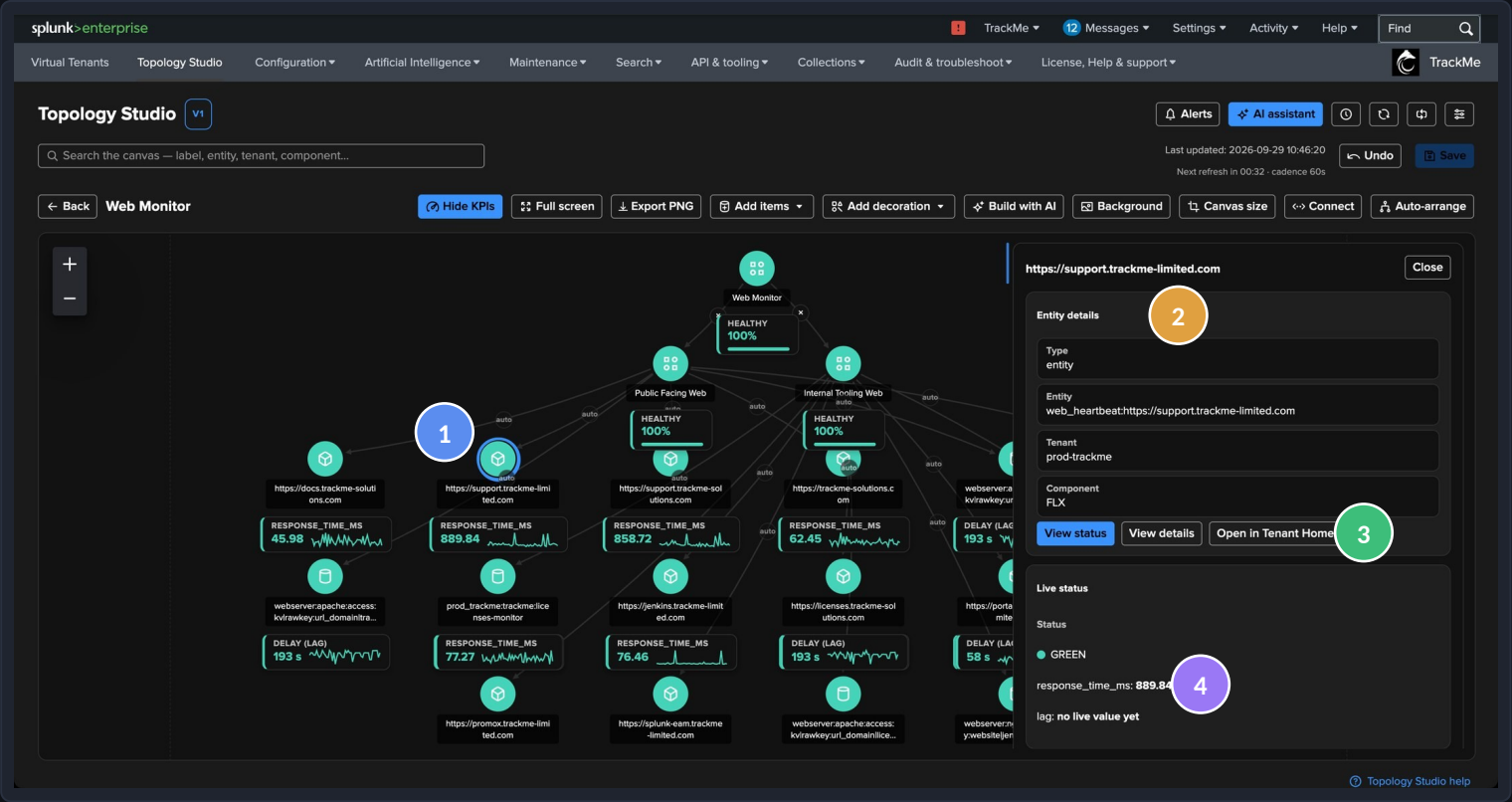
Add aggregate

- 1 Show and link members
Matching entities are drawn and linked around the aggregate.
- 2 Only entities in alerts
Optional: draw red members only.
- 3 Auto-entities filter
What is drawn — never what is measured.
- 4 Max entities shown
Up to 500; beyond, "+N more".
- 5 Default KPIs
Up to five per member, from the scope's catalog: response_time_ms, lag...
- 6 Sparkline
Label, value and a 24-hour trend.



Every save is a version. Undo covers the last 25 operations.

Click any node — the inspector explains it



- 1 A generated member
One of the heartbeat checks of Public Facing Web.
- 2 Entity details
Entity, tenant and component — here an FLX entity.
- 3 View status · View details · Open in Tenant Home
From the map to the status message, the entity and its tenant.
- 4 Live status
State and the current value of each KPI.

03

PART 3 • ALERT

Alert on the service the map draws

A Topology Alert evaluates the nodes of a view on a schedule and notifies on transitions only — with the rendered map in the email.

A Topology Alert on Web Monitor

Create topology alert

Alias *

Web Monitor health

Alert ID: web-monitor-health — unique identifier, cannot be changed later.

View *

Web Monitor (web-monitor)

Only views you can edit are offered — managing alerts on a view requires write access. The view cannot be changed after creation.

Schedule (cron) *

* / 15 * * * *

5-field cron, e.g. */15 * * * *.

Also alert on orange

By default only red items raise the alert, enable to treat orange as alerting too. Missing references are reported but do not alert.

Event index

Deployment default (trackme_summary)

Where this alert's transition events are written, as sourcetype="trackme: topology_alerts". A topology view spans tenants, so the target belongs to the alert rather than to a tenant. Leave on the default unless you route topology alerting to its own index.

Delivery

Send email on transitions

An event is always emitted on every transition.

Email account *

smtp-relay

prodtest@trackme-limited.com

Type an email address and press Enter to add it. At least one recipient is required.

Topology image theme

Dark

Theme of the topology image embedded in emails.

Cancel

Create alert

Edit topology alert — Web Monitor health

Email account *

smtp-relay

Recipients *

prodtest@trackme-limited.com

Type an email address and press Enter to add it. At least one recipient is required.

Topology image theme

Dark

Theme of the topology image embedded in emails.

Drilldown root URL (optional)

Auto-detected from the server

Root URL of Splunk Web used to compose the "Open the topology view" link in emails. Leave empty to use the auto-detected server URL — set it when Splunk is reached through a reverse proxy or a custom domain.

Selection *

Automatically select all entities, aggregates and views

The alert covers every entity, aggregate and referenced view — including nodes added in the future, without updating the alert.

Filter nodes by name, entity, tenant or component...

All 3 alertable nodes selected automatically — nodes added to the view later are covered without updating the alert.

AGGREGATES

Web Monitor

prod-trackme (dhm, dsm, flx) — filter: priority IN ("high", "critical") AND labels IN ("public-facing", "internal-tooling")

selected

Public Facing Web

prod-trackme (dhm, dsm, flx) — filter: priority IN ("high", "critical") AND labels IN ("public-facing")

selected

Internal Tooling Web

prod-trackme (dhm, dsm, flx) — filter: priority IN ("high", "critical") AND labels IN ("internal-tooling")

selected

Enabled

Cancel

Update alert

1

Alias
The alert id is derived from it.

2

View
Views you can edit only.

3

Schedule
A cron — every 15 minutes by default.

4

Also alert on orange
Off by default: only red opens.

5

Email on transitions
A TrackMe email account, recipients, image theme.

6

Selection
Every node, including nodes added later — or a list.

TrackMe for Splunk · Hands-on: Topology Studio

docs.trackme-solutions.com

Every alert, its state, its runs

Topology alerts

Topology alerts are scheduled, state-aware evaluations of the nodes of a topology view: they notify on transitions only — open on breach, update when the set of unhealthy items changes, resolve on recovery. An event is always emitted on every transition; email is an opt-in delivery channel on top.

Events land in index="trackme_summary" sourcetypes="trackme:topology_alerts" — each alert chooses its own target index.

Showing all alerts — show only "Web Monitor"

Alias	View	Selection	Enabled	Status	Last / Next run	Duration	Owner	Cron	Actions
SecOps Full	secops-view-references	All nodes (auto)	Enabled	ALERT (7 items)	Last: 29/09/2026, 10:48:39 (6m ago) Next: 29/09/2026, 11:03:28 (in 8m)	Max 14.9s Avg 8.4s Last 9.9s	gmarchand	* / 15 * * * *	:
TrackMe Production	trackme-production	All nodes (auto)	Enabled	ALERT (6 items)	Last: 29/09/2026, 10:54:22 (46s ago) Next: 29/09/2026, 10:59:18 (in 4m)	Max 9.3s Avg 4.8s Last 2.7s	gmarchand	* / 5 * * * *	:
TrackMe Production Web	trackme-production-web	All nodes (auto)	Enabled	OK	Last: 29/09/2026, 10:51:45 (3m ago) Next: 29/09/2026, 10:56:42 (in 2m)	Max 3.8s Avg 2.2s Last 2.0s	gmarchand	* / 5 * * * *	:
Web Monitor health	Web Monitor	All nodes (auto)	Enabled	OK	Last: 29/09/2026, 10:55:04 (4s ago) Next: 29/09/2026, 11:10:02 (in 15m)	Max 2.1s Avg 1.7s Last 1.2s	gmarchand	* / 15 * * * *	:

+ New alert

Events (all views)

Close

Run history — TrackMe Production

Runs: 50

Fired: 0

Duration avg: 4.8s

Duration max: 9.3s

When	Transition	Items	Email	Duration	Error
29/09/2026, 10:44:25	None	6 in alert	—	6.0s	—
29/09/2026, 10:39:23	None	6 in alert	—	4.7s	—
29/09/2026, 10:34:26	None	6 in alert	—	6.9s	—
29/09/2026, 10:29:23	None	6 in alert	—	3.8s	—
29/09/2026, 10:24:21	None	6 in alert	—	3.1s	—
29/09/2026, 10:19:24	None	6 in alert	—	4.7s	—
29/09/2026, 10:14:25	None	6 in alert	—	6.2s	—
29/09/2026, 10:09:25	None	6 in alert	—	5.7s	—
29/09/2026, 10:04:22	None	6 in alert	—	3.7s	—
29/09/2026, 09:59:23	None	6 in alert	—	4.1s	—
29/09/2026, 09:54:24	None	6 in alert	—	5.6s	—
29/09/2026, 09:49:24	None	6 in alert	—	4.7s	—
29/09/2026, 09:44:24	None	6 in alert	—	5.4s	—
29/09/2026, 09:39:23	None	6 in alert	—	3.5s	—
29/09/2026, 09:34:24	None	6 in alert	—	5.1s	—
29/09/2026, 09:29:22	None	6 in alert	—	3.3s	—
29/09/2026, 09:24:22	None	6 in alert	—	3.8s	—

Back

1 Web Monitor health

The new alert, run once: OK.

2 ALERT (n items)

Alerts currently open, with the number of items in alert.

3 Last / next run

Durations and schedule at a glance.

4 Events

The trackme:topology_alerts events, pre-scoped.

5 Transition: None

While nothing changes, no notification — the alert stays quiet.

6 Items in alert

Recorded on every run, with email delivery and duration.

The email — the map itself, where the red is

TrackMe

Topology Alert — TrackMe Production

Alert: trackme-production
View: trackme-production
Transition: open

ALERT OPENED — TrackMe Production

[Open the topology view in TrackMe](#)

Topology view: TrackMe Production · Status: **RED** · Since: 2026-09-22 15:49:32 UTC

Items in alert (2)

State	Item	Type	Detail
RED	TrackMe Prod	aggregate	18 entities (green: 16, red: 2)
RED	Internal Tooling	aggregate	6 entities (green: 2, red: 4)

Topology

- Alert opened**
Transition open, status red, and since when.
- Items in alert**
Which aggregates are red, how many entities, how many of them red.
- The topology**
Rendered on the server with the same icons and KPIs — red nodes where the problem is.
- Drilldown**
Open the topology view in TrackMe, straight to the live map.

One thread per incident

Open, update when the set of affected items changes, resolve on recovery — never a repeat while nothing changes.

Resolved — back to green, with the duration

TrackMe

Topology Alert — TrackMe Production

Alert trackme-production
View trackme-production
Transition resolve

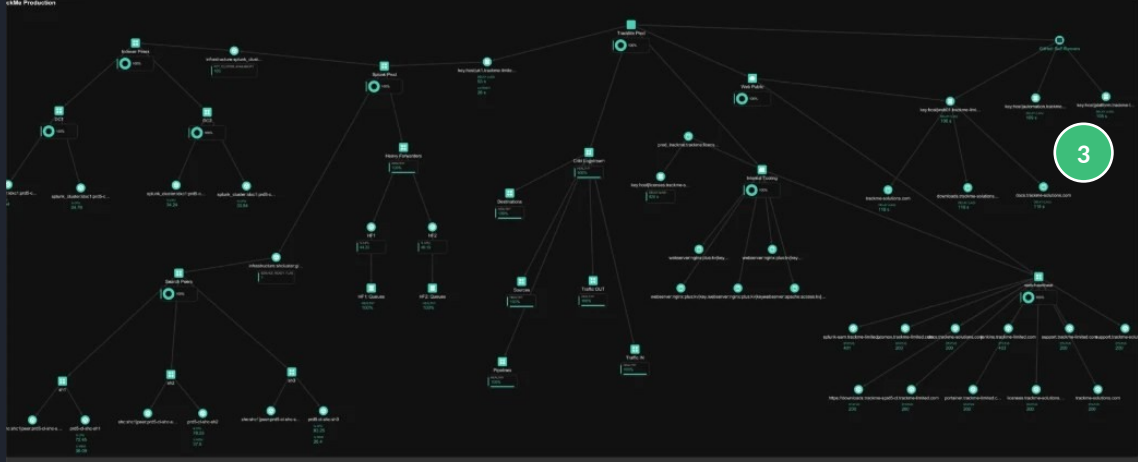
ALERT RESOLVED — TrackMe Production 1

[Open the topology view in TrackMe](#)

Topology view: TrackMe Production · Status: **GREEN** · Was in alert since: 2026-09-26 06:34:25 UTC — resolved after 1h 55m 2

All selected items are healthy again.

Topology



This is an automated email, please do not reply directly to this email.

1

Alert resolved

Transition resolve, status green.

2

How long it lasted

In alert since... resolved after 1h 55m — the incident duration, measured.

3

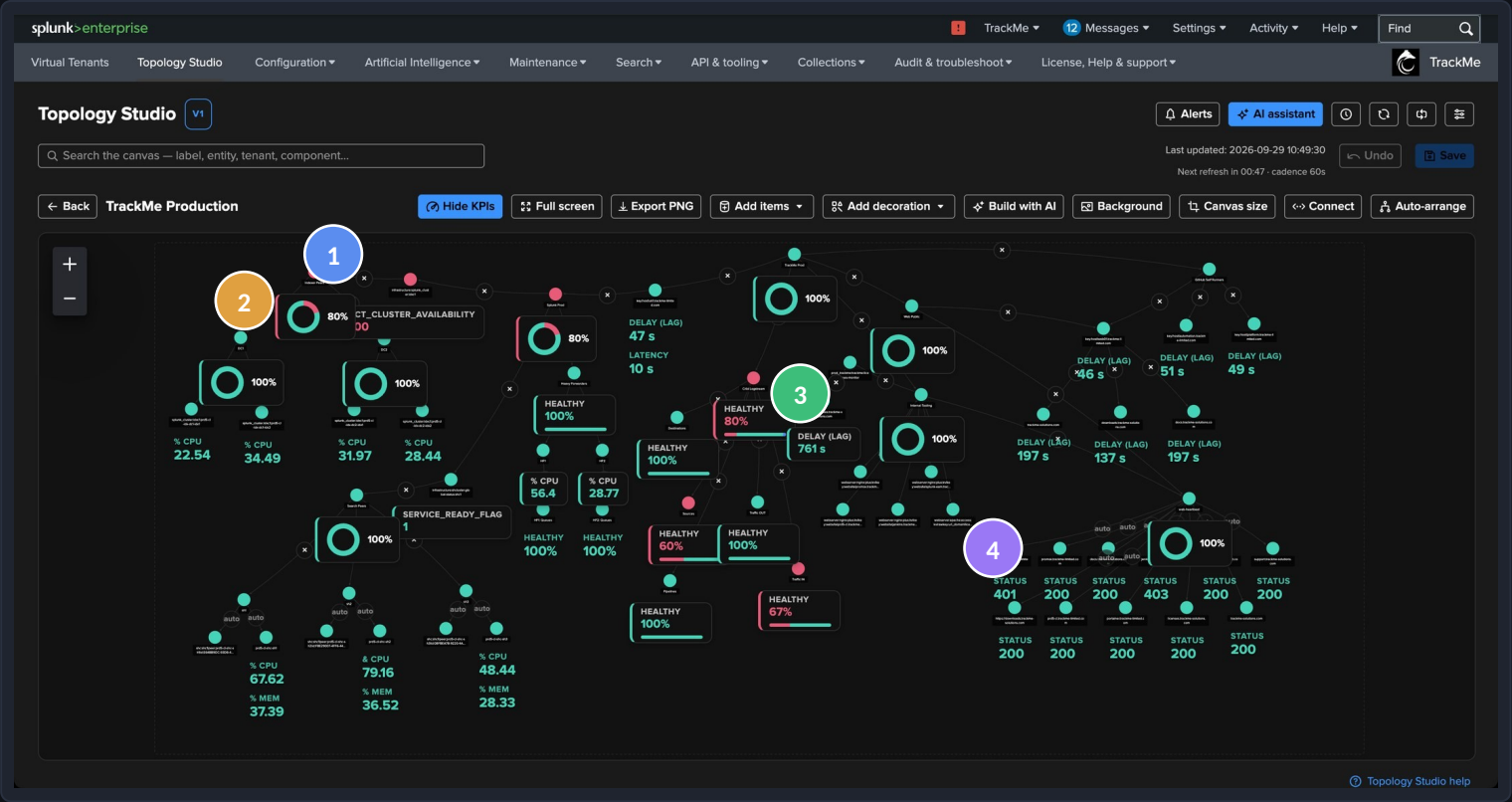
All green again

The same rendered map, every node back to healthy.

Honest by design

Missing nodes never alert; unavailable data freezes the state; a maintenance window pauses the evaluation instead of resolving it.

The same map, live — where the red is



- 1 Red members
Drawn by their aggregates, worst states first.
- 2 Donut KPIs
Member-state distribution of an aggregate.
- 3 Aggregates in alert
Healthy percentage below the threshold.
- 4 Entity KPIs
CPU, memory, delay — the numbers behind the colours.

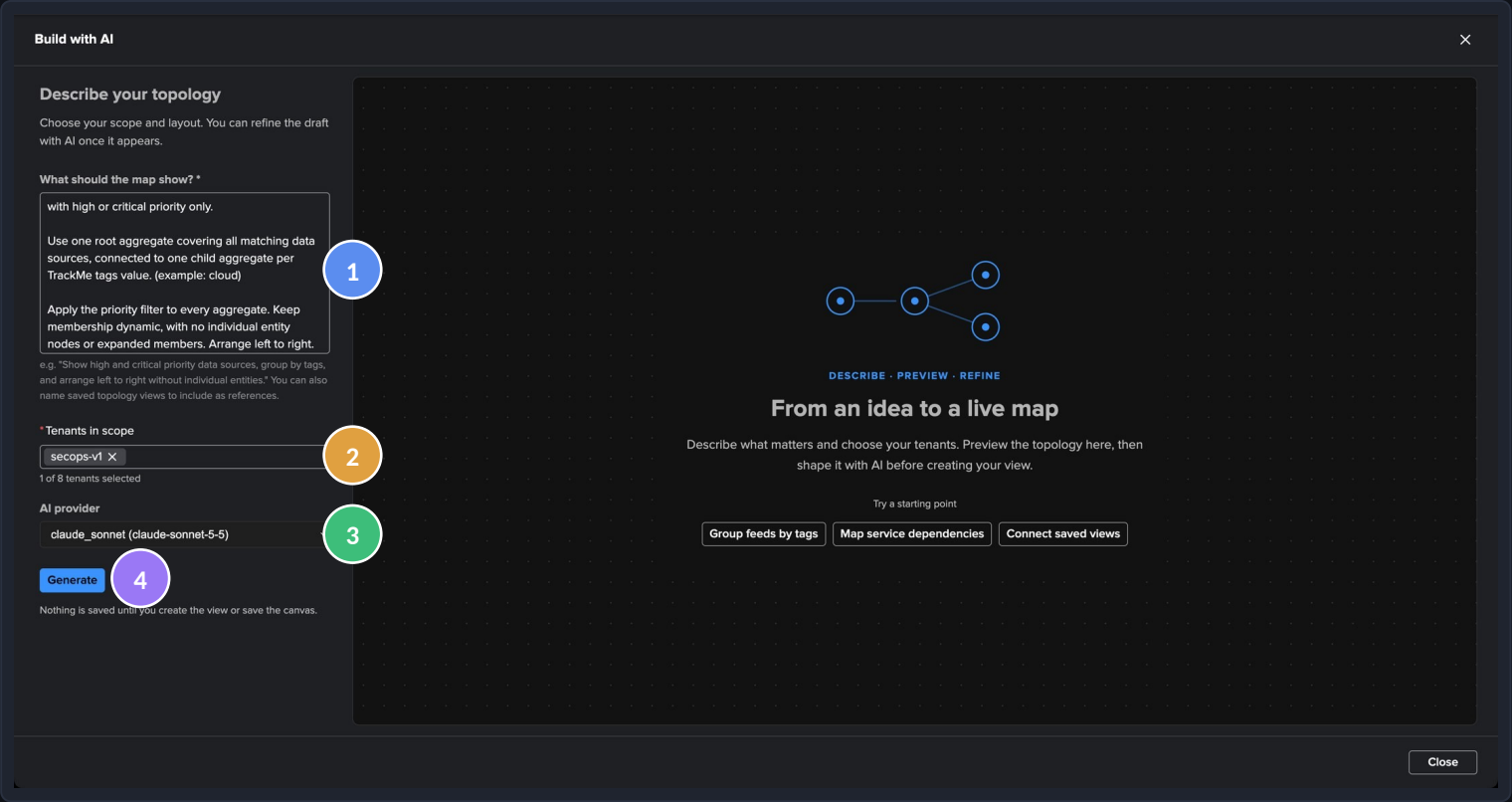
04

PART 4 • AI

Describe the map — let the AI build the draft

Build with AI turns a sentence into a live draft on a preview canvas. You refine it in plain words, then create the view. Nothing is saved until you do.

Build with AI — one prompt, a tenant, a provider



1 What should the map show?

A “SecOps Feeds” topology for high and critical DSM entities, one root aggregate, one child per TrackMe tags value, dynamic membership, no individual entities, left to right.

2 Tenants in scope

Up to eight: secops-v1 here.

3 AI provider

Any configured provider — Claude Sonnet here.

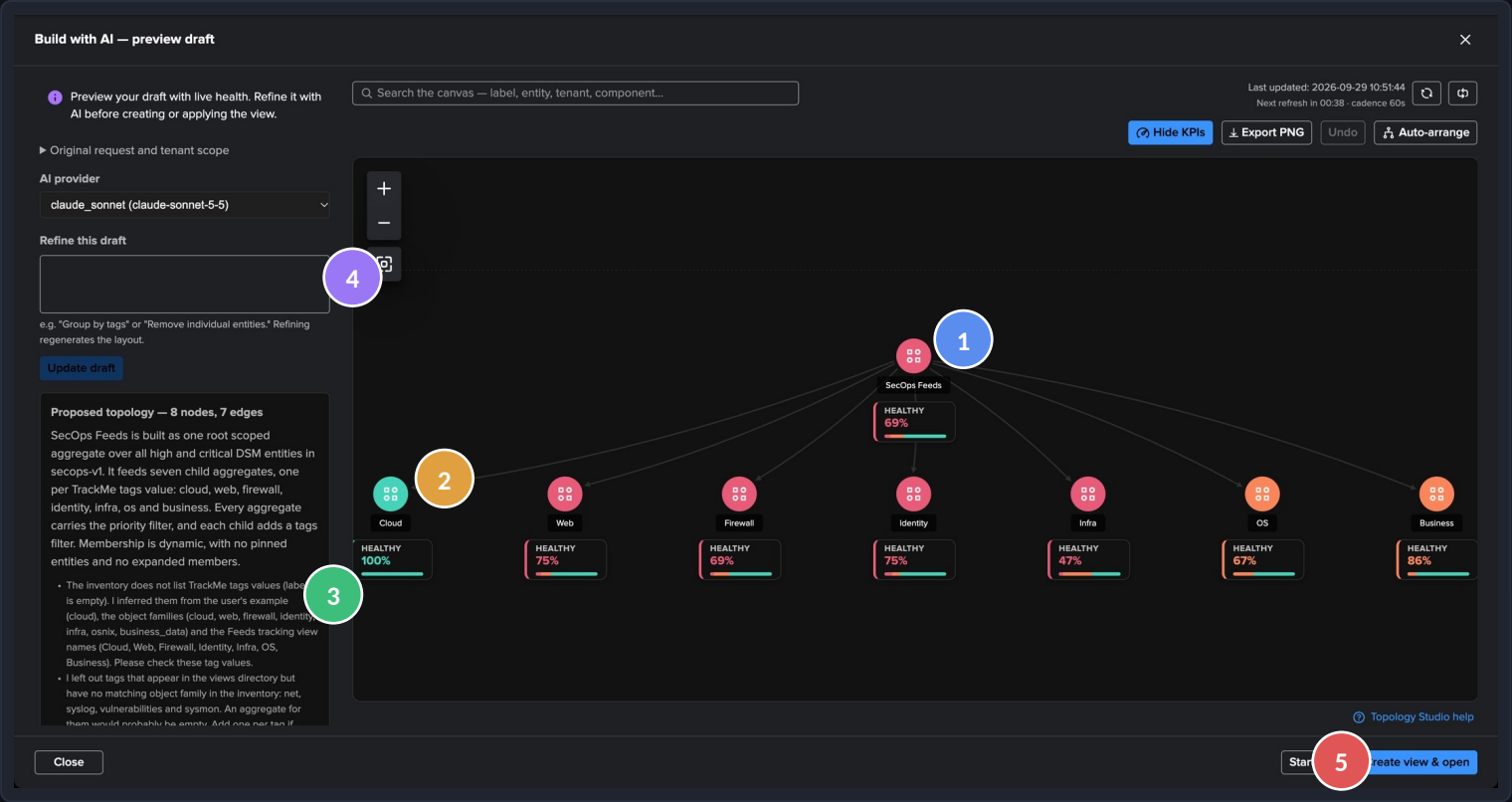
4 Generate

The builder streams its progress; nothing is saved.

Starting points

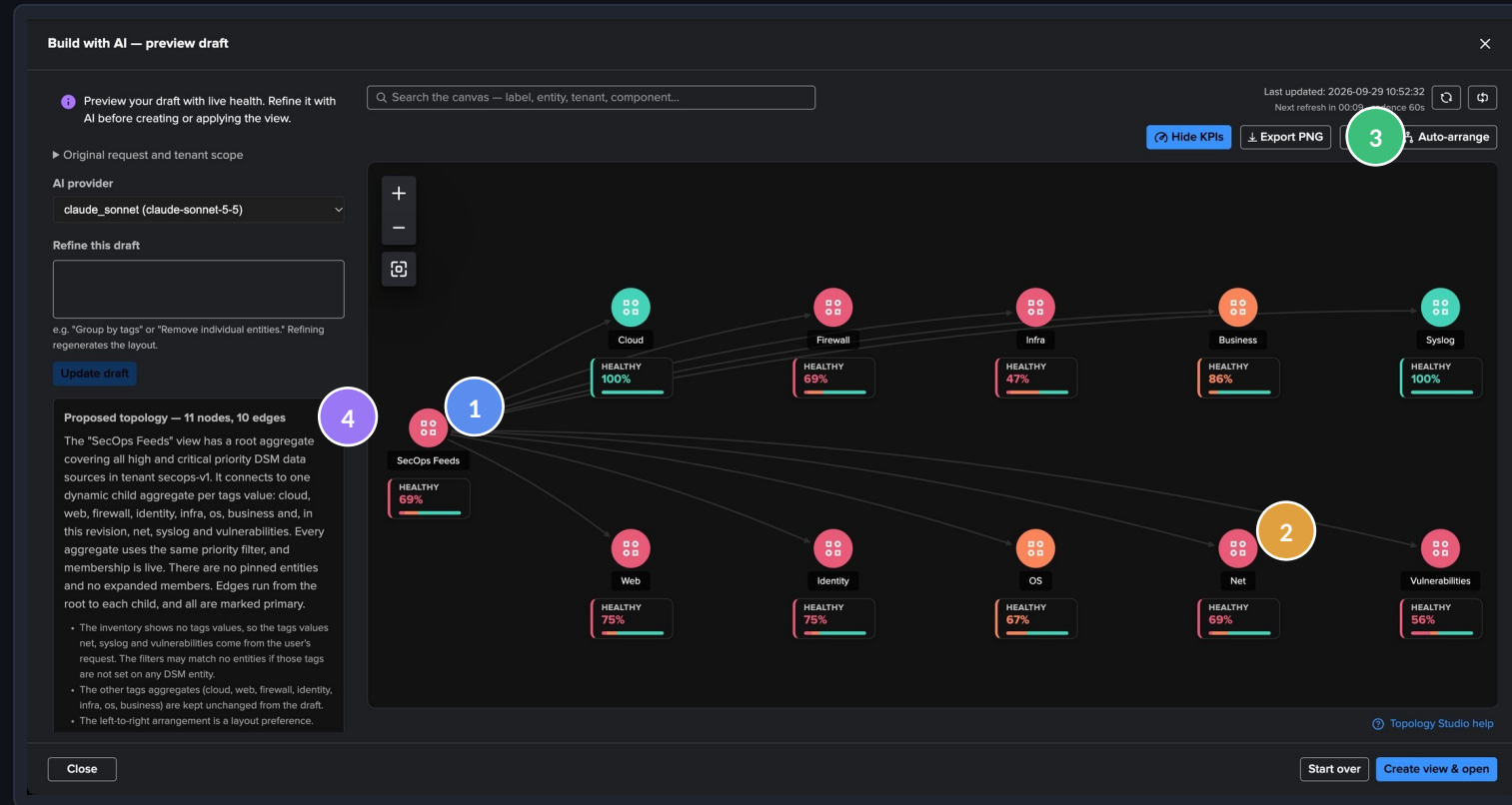
Group feeds by tags · Map service dependencies · Connect saved views — ready prompts on the empty canvas.

The draft — live health, and the AI says what it assumed



- 1 SecOps Feeds**
The root scoped aggregate over high and critical DSM entities.
- 2 One child per tag**
cloud, web, firewall, identity, infra, os, business — each with the priority filter.
- 3 What it assumed**
The inventory lists no tag values: it inferred them — and says so.
- 4 Refine this draft**
Follow-up instructions in plain words.
- 5 Create view & open**
Only then is anything saved.

Refine in plain words, arrange left to right



1 The root

Unchanged — refining regenerates the draft, not your intent.

2 net, syslog, vulnerabilities

"Also add child aggregates for the net, syslog and vulnerabilities tags values" — done.

3 Auto-arrange

Left to right, spacious: the layout direction is a canvas setting.

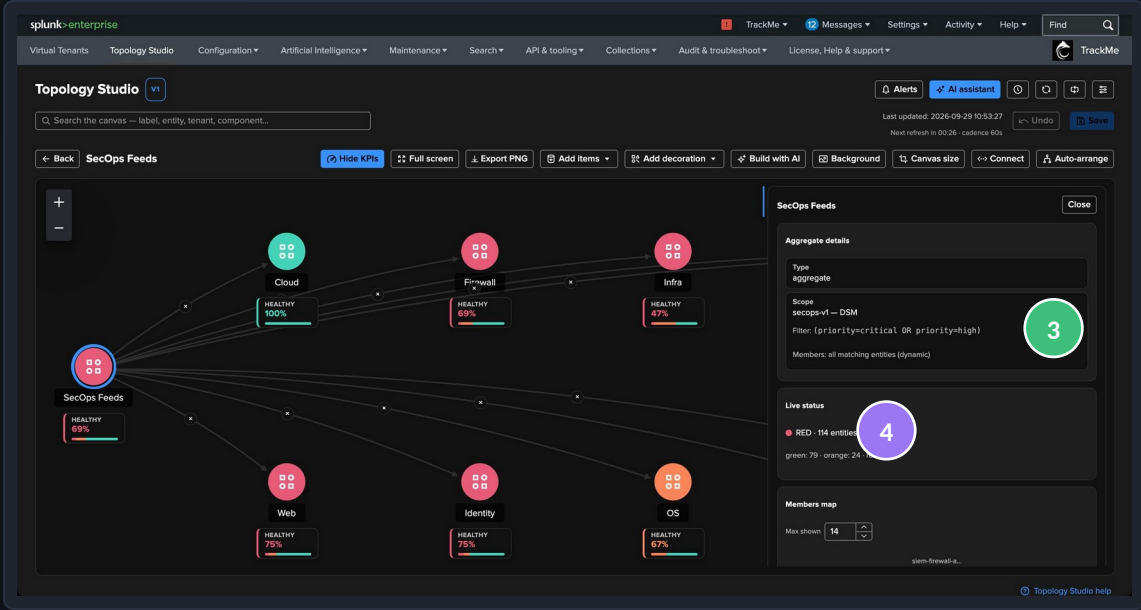
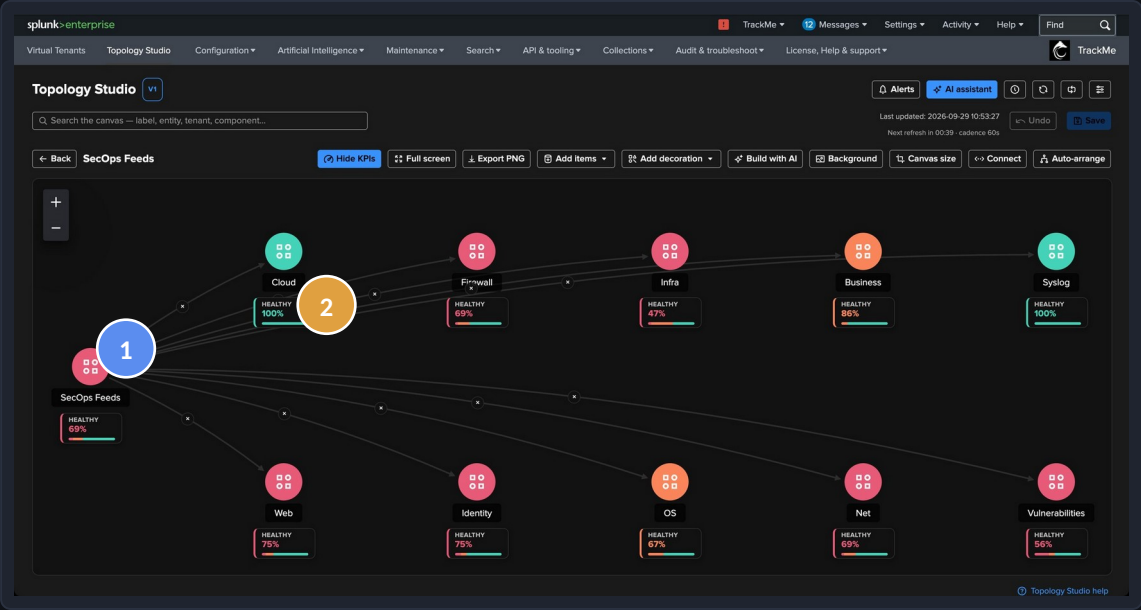
4 11 nodes, 10 edges

The updated summary of the draft.

Good to know

The builder always lays out top-down; the direction is one click in Auto-arrange. For a guaranteed split by tag, the Tenant Home hierarchy of Part 1 is the other road to the same map.

Created — a view like any other



1 SecOps Feeds

Saved, opened, with live health on every node.

2 Children with KPIs

Healthy percentage per tag.

3 Scope and filter

secops-v1 · DSM · priority critical or high — dynamic membership.

4 Live status

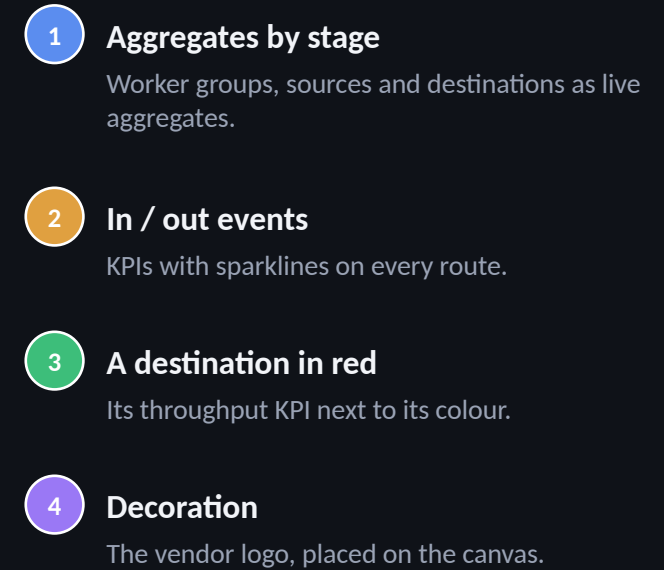
The same entities as the Tenant Home map of Part 1.

05

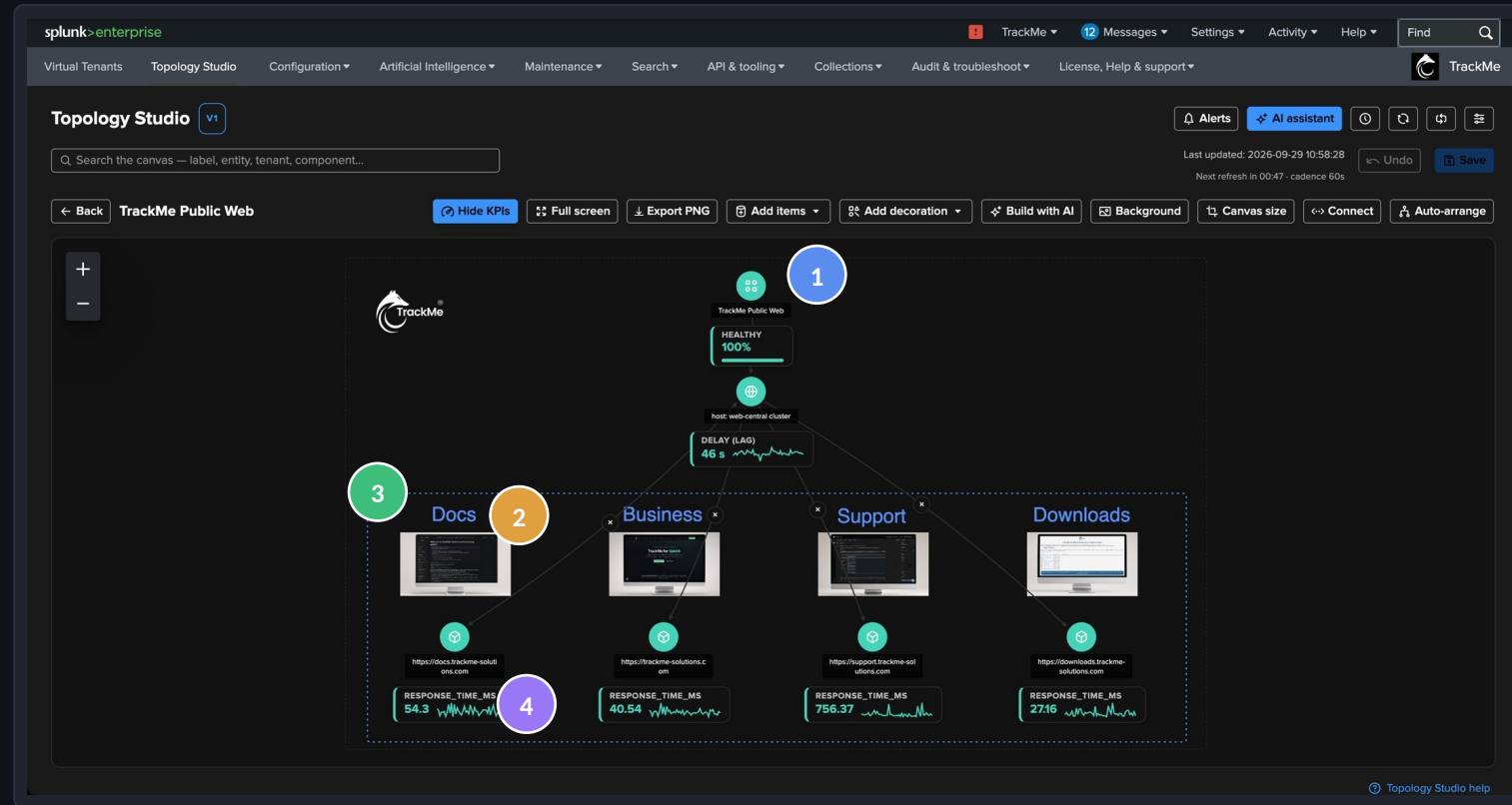
IN PRODUCTION

Maps that run every day

A Cribl pipeline, a public web estate, and a map of maps over the Splunk infrastructure — with a drilldown from the top view to the reason.



A public web estate — screenshots as decorations



1 The estate

One aggregate over the public web properties.

2 Image decorations

A screenshot of each site above its heartbeat check.

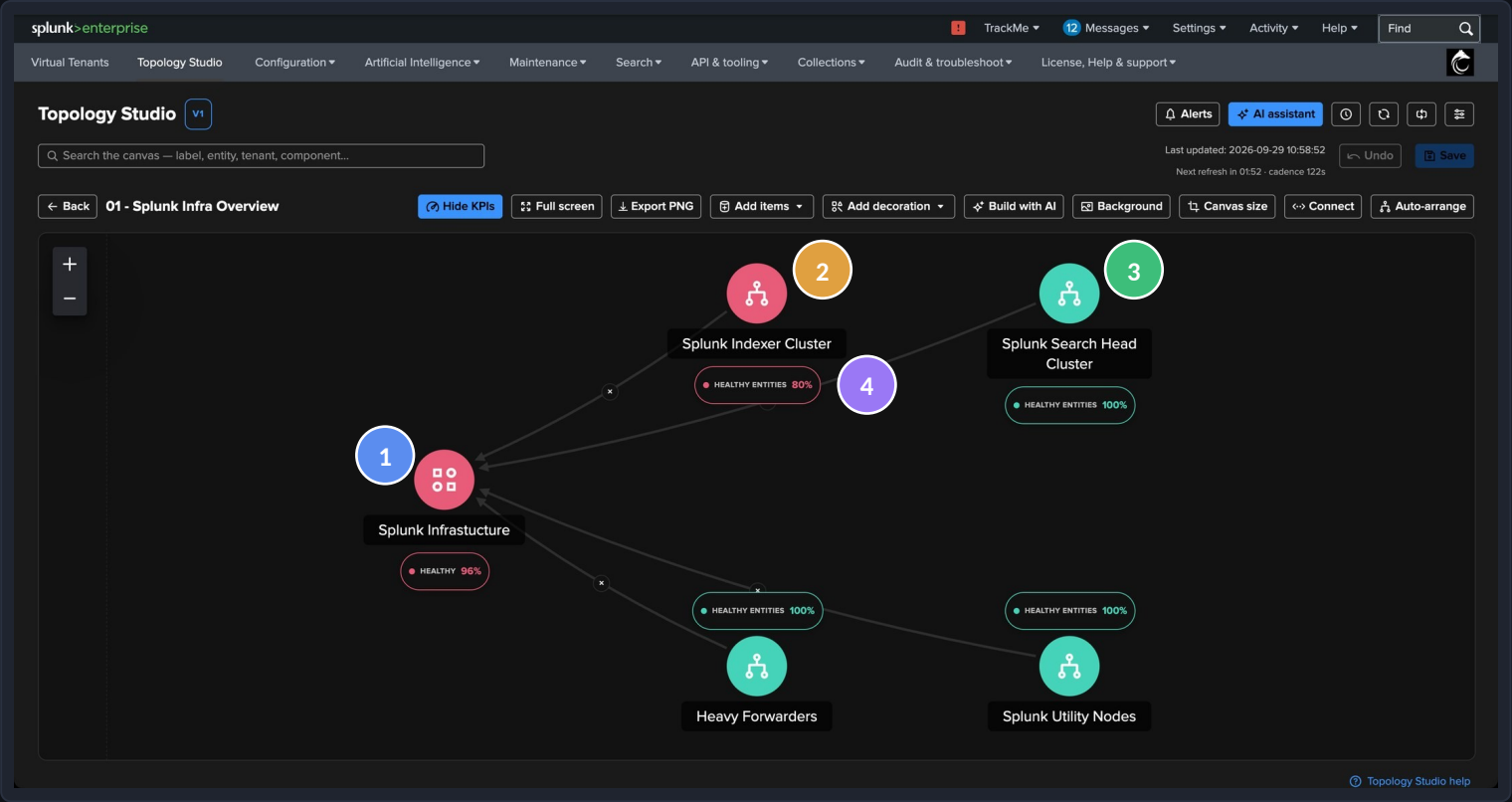
3 Shapes

A dashed zone around the web front ends.

4 Response time

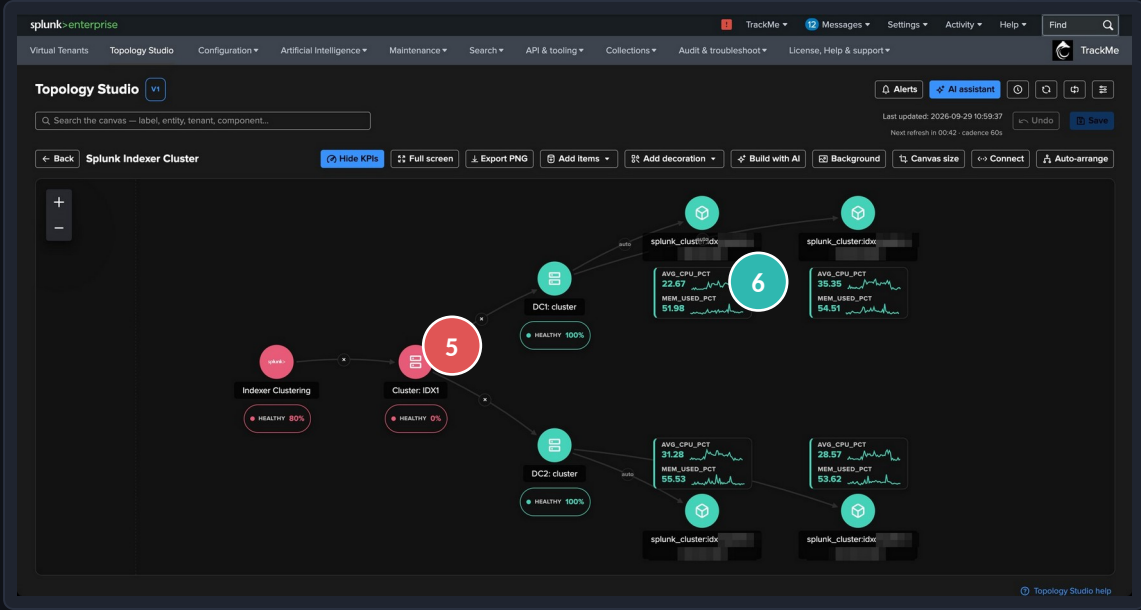
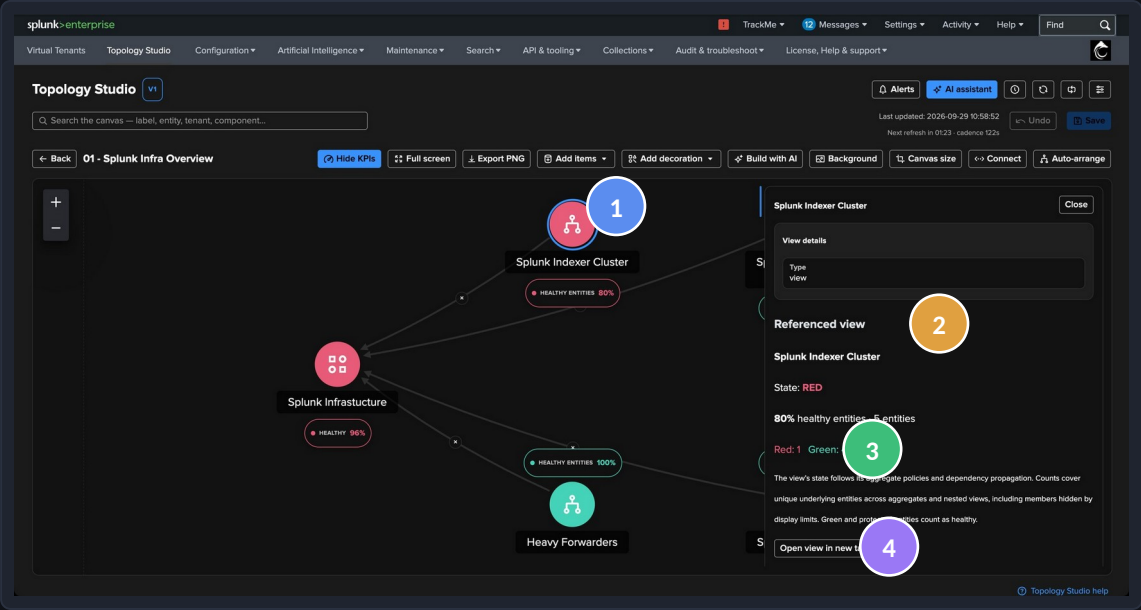
Sparkline KPIs on every heartbeat.

A map of maps — the Splunk infrastructure at a glance



- 1 **Splunk Infrastructure**
An aggregate over the whole platform.
- 2 **A view node in red**
The Splunk Indexer Cluster view, folded into one node.
- 3 **Other views**
Search head cluster, heavy forwarders, utility nodes — each its own map.
- 4 **Healthy entities**
Unique entities across the nested views, counted once.

Drill down — from the view node to the view



- 1 The red view node**

Splunk Indexer Cluster, selected.
- 2 Referenced view**

Its state and healthy entities.
- 3 Red: 1 • Green: 4**

Unique entities of the nested view.
- 4 Open view**

Straight into the referenced map.
- 5 Cluster: IDX1**

The red node inside: the cluster itself.
- 6 Peers and sites**

All healthy, with CPU and memory sparklines.

View status — the reason, in plain words

Entity status

infrastructure:splunk_cluster:idxc1

Entity status

State: red

Impact score: 100

Status message:

Status conditions not met

Raw JSON

The entity status is not complying with monitoring rules (status: 2, status_description: Some peers are down/unknown or the cluster status is not ready, cluster_readiness: [{"available_sites":["site1,site2"],"maintenance_mode":"0","multisite":"1","rolling_restart_flag":"0","service_ready_flag":"1"}], peers_summary: {peers-up: 4, peers-down: 0, peers-unknown: 0, health_summary: {"all_data_is_searchable":"1","all_peers_are_up":"1","no_fixup_tasks_in_progress":"1","replication_factor_met":"0","search_factor_met":"0","site_replication_factor_met":"0","site_search_factor_met":"0"}})

IMPACT SCORE BREAKDOWN

Contribution	Detail	Score
Base score	Score events over the last 24 hours	0
Status conditions not met	Status not met	+100
Total impact score		100

ADDITIONAL DETAILS

extra_attributes.cluster_status_summary [{"available_sites":["site1,site2"],"maintenance_mode":"0","multisite":"1","rolling_restart_flag":"0","service_ready_flag":"1"}]

extra_attributes.cluster_config_summary [{"replication_factor":"3","search_factor":"2","site_replication_factor":{"origin":2,total:3},"site_search_factor":{"origin":1,total:2}}]

extra_attributes.cluster_peers_summary [{"peers-up":4,"peers-down":0,"peers-unknown":0,"health_summary":{"all_data_is_searchable":"1","all_peers_are_up":"1","no_fixup_tasks_in_progress":"1","replication_factor_met":"0","search_factor_met":"0","site_replication_factor_met":"0","site_search_factor_met":"0"}}]

View details

Open in Tenant Home

Close

- 1

Status message

Some peers are down or the cluster is not ready: replication factor and search factor not met.
- 2

Impact score breakdown

Status conditions not met: +100 — red.
- 3

Raw JSON

The structured status behind the view.
- 4

Additional details

Cluster status, configuration and peers summaries — the evidence.
- Three clicks

From the top view of the platform to the exact reason: view node, cluster, View status.

Where we are

In four parts

● Generated

a map of a tenant from Tenant Home — per index, then per tag, narrowed to high and critical, saved as a view

● Authored

Web Monitor from an empty canvas: a root aggregate, two children by label, members drawn with KPIs and sparklines

● Alerted

a Topology Alert on the view: transitions only, the rendered map in the email, runs and events recorded

● Built with AI

SecOps Feeds from one prompt, refined in plain words, arranged left to right, created as a view

What made it work

Made of real entities

Every node is a TrackMe entity, aggregate or view — the map cannot drift from what is monitored, and it colours itself.

Membership that follows

Aggregates are filters, not lists: new matching entities join, retired ones leave, and members draw themselves.

Alerts on the service

Transitions only, frozen during maintenance and data gaps, with the map in the email — one signal per service.