PA NUG

Network observability

Dashboards for the decisions people make

Josh VanDeraa / October 2026

Presented By:
(US)NUA
US Networking User Association

Josh VanDeraa

Network engineering and automation

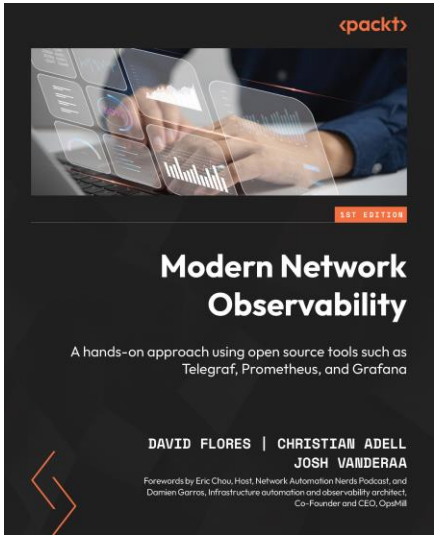
20+ years in networking

Enterprise retail, travel,
managed services, and consulting

josh-v.com



Author



Co-author / Packt

A reachable network, a slow service

A branch reports intermittent application delays.

The router still answers. Other sites look normal.

What would you look at next?

Network evidence

Question	Evidence	Important limit
How much, and when?	Metrics	Collection intervals hide short events
What changed?	Logs and configuration history	An event is not proof of cause
Who is using the path?	Flow records	Sampling limits detail
Which path and neighbors?	State and topology	Snapshots can be stale
Can the service respond?	Active service checks	The probe represents one vantage point

Dashboard audiences

Audience	Decision	Typical horizon
Executives	Which critical services are available?	Current impact and monthly trends
Service owners / SRE	Which application behavior changed?	Incident window and baseline
Network operations	Which network dependency is impaired?	Now and the current shift

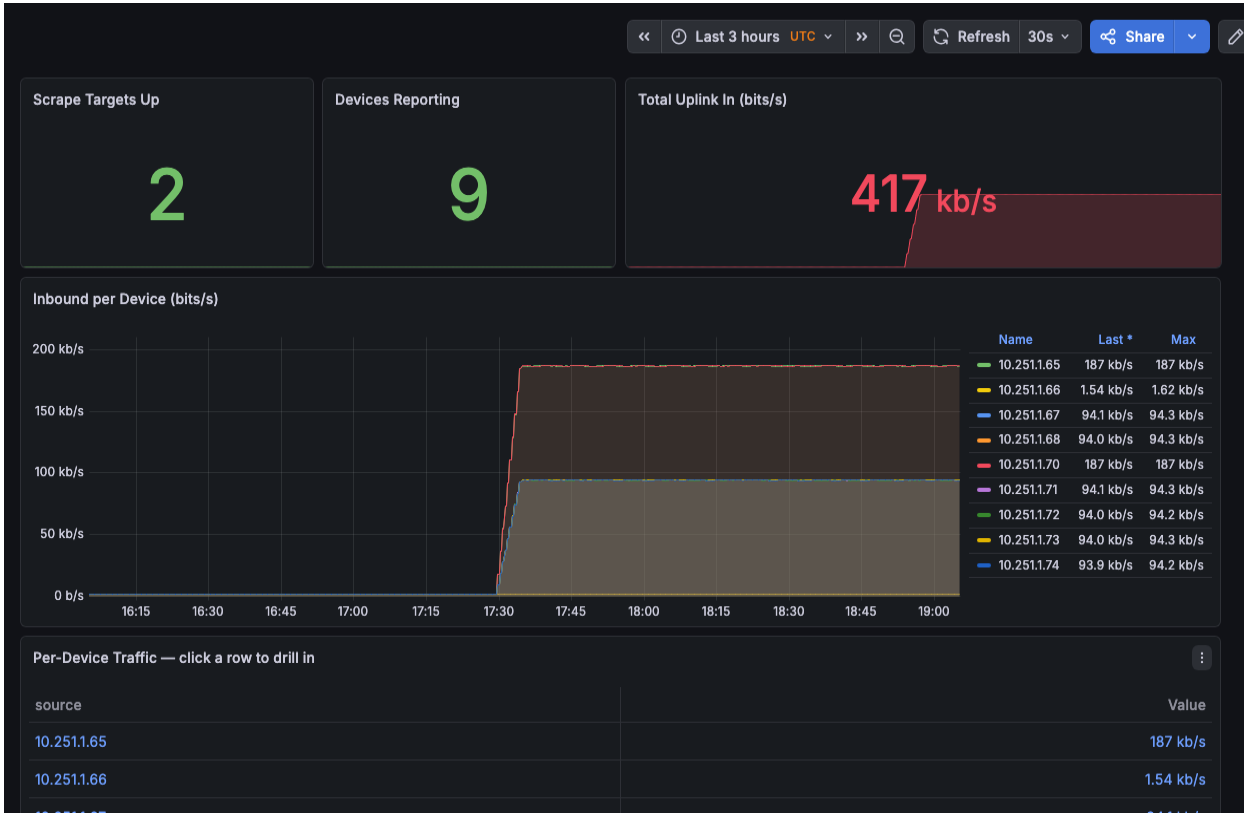
The OSNM Grafana walkthrough

Operations: fleet traffic and a device to investigate.

Engineering: interface detail and log events.

Dashboard design: the evidence each audience needs.

Grafana: fleet overview



Operations

9 devices reporting

2 scrape targets up

Next: a device row

OSNM lab / Fleet Overview

Operations: the next investigation

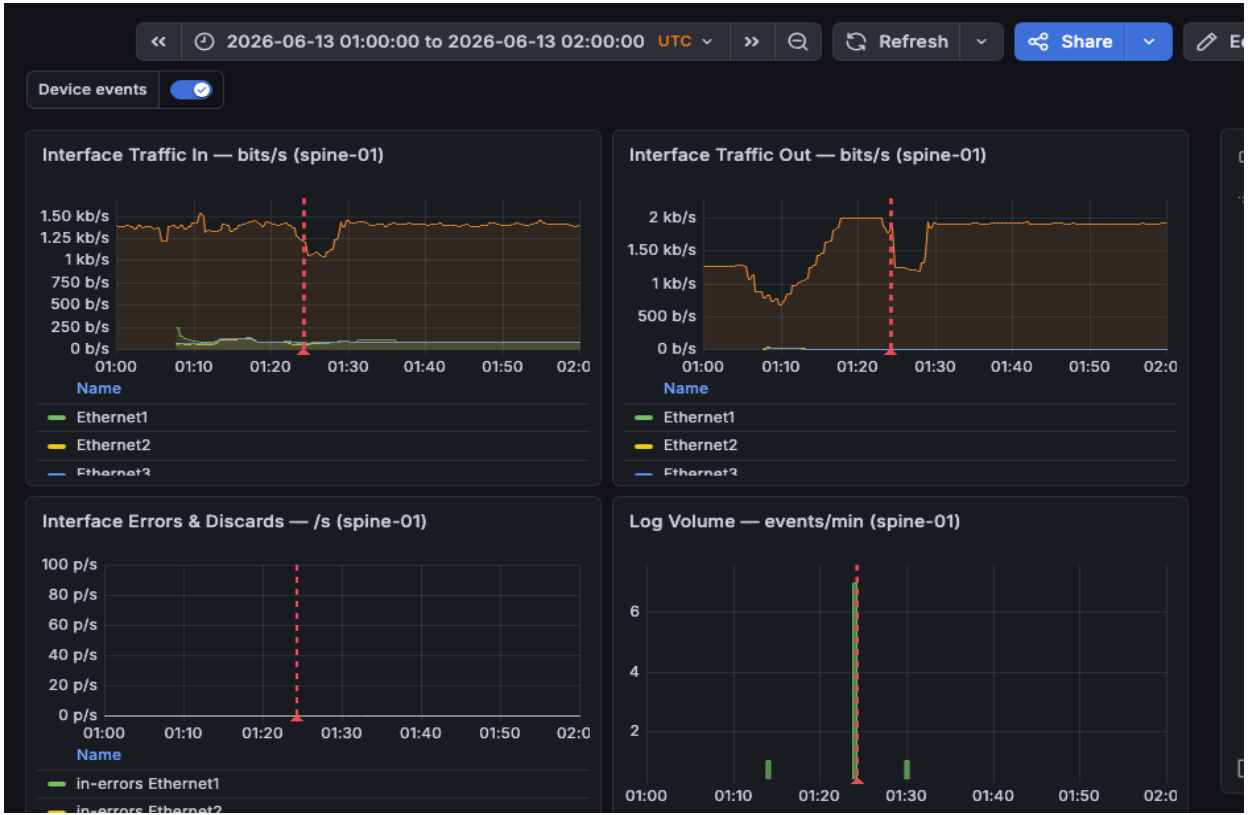
A traffic change identifies a place to investigate.

The device link should preserve the time range.

A successful scrape confirms one part of the pipeline.

Service impact needs a service check and an owner.

Grafana: device drill-down



Engineering

Traffic by interface

Events near 01:24

Errors and log volume

OSNM lab / spine-01 / June 13, 01:00–02:00 UTC

The event and the next test

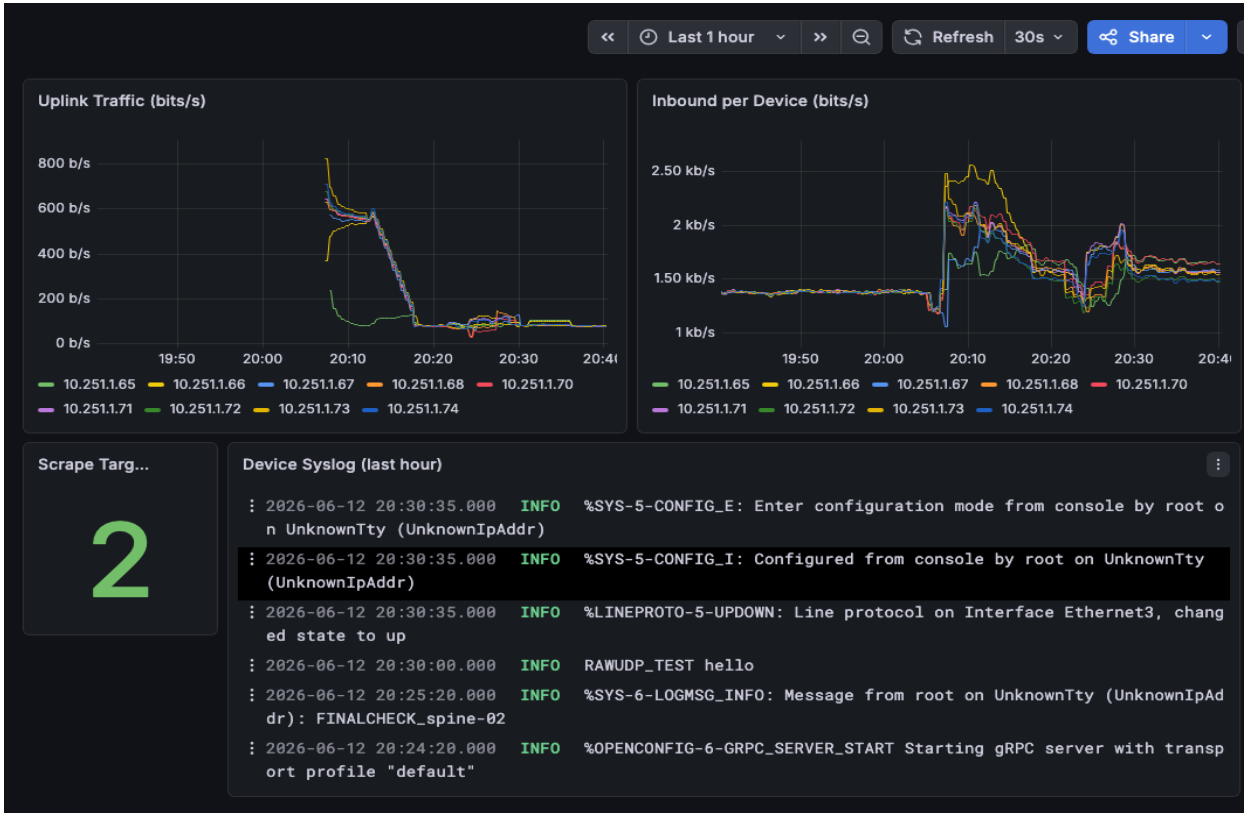
01:24:20 UTC: link and BGP events in the book lab.

The log-volume spike gives us a time to investigate.

Traffic changes provide context for the event.

A service check would tell us whether users recovered.

Grafana: dashboards by audience



Operations

Traffic beside syslog

Engineering

A device and event

Leadership needs

Service impact + owner

OSNM lab / Network Overview

Executives: service availability

Critical services: available, degraded, unavailable, or unknown.

Affected locations and business functions, with an owner.

Availability against a stated target and reporting period.

Next view: the application behind the affected service.

Service owners: application health

Dashboard evidence	Measure or context	Next investigation
Requests and responses	Volume, success rate, error codes	Affected endpoint or operation
Response time	p50 / p95 latency and target	Slow operation or dependency
Application logs	Errors and deployment events	Request or trace correlation
Critical dependencies	DNS, identity, database, networks	Dependency health and owner

Networks behind the service

Network question	Evidence	Application context
Availability and reachability	Service probes over a defined period	Location and endpoint
Is the path degraded?	Loss, round-trip time, link state	Circuit and routing context
Is capacity constrained?	Utilization, errors and discards	Interface role and capacity
Which services may be affected?	Affected resource and timestamp	Related applications and owners

One application and its dependencies

Order entry example	Modeled dependency	Operational evidence
Name resolution	Corporate DNS service	Lookup success and duration
User sign-in	Identity provider	Authentication success and latency
Order storage	Database service and endpoint	Connections, errors and query time
Network access	VRF, prefixes, VLANs, circuits	Path probes and network metrics

Application context from Nautobot

Proposed catalog: application ID, owner, criticality, environment.

Relationships: supporting services and network resources.

API-fed context keeps Grafana filters and links consistent.

Telemetry supplies observed health, with freshness visible.

Shared identity and context

Raw signal	Shared context	Used by
192.0.2.65 in metrics	device = spine-01	Device drill-down
spine-01 in logs	device = spine-01	Shared event timeline
Interface identifier	site, circuit, role, capacity	Impact and capacity views
Service check	service, site, owner	Leadership and operations

Missing evidence

A quiet log stream may be healthy, broken, or simply untested.

Show last observation and expected collection cadence.

Use a heartbeat or delivery test where silence is ambiguous.

Treat unknown service health as unknown.

Actionable alerts

State the affected service or resource.

Include a time window and a link to the evidence.

Route to someone who can act.

Verify both the failure and the recovery behavior.

The OSNM implementation

Capability	Book example	Contribution
Inventory and context	Nautobot	Identity, location, device and interface roles
Collection	Telegraf	SNMP and gNMI metrics
Storage	VictoriaMetrics / VictoriaLogs	Queryable metrics and events
Visualization and alerting	Grafana	Views, drill-downs, notifications

Sonda demo design

One synthetic application, viewed by every persona.

A network failure changes a service probe and related metrics.

Shared application IDs join logs and network dependencies.

Failure, recovery, and missing data exercise each dashboard.

A first useful dashboard

Choose one recurring operational question and its audience.

Identify the signals and context needed to answer it.

Build the view and its next drill-down.

Exercise a failure, recovery, and missing-data case.

Your next dashboard

Name the person who needs it.

Name the question they need answered.

Name the evidence you are missing.