Business Activity Monitoring with Nagios

Anders Håål
Ingenjörsbyn AB

Business activity monitoring - BAM

*The goals of business activity monitoring are to provide **real time information** about the status and results of various business related operations, processes, and transactions.*

*The main benefits of BAM are to enable an enterprise to make better **informed business decisions**, **quickly address problem** areas, and **re-position organizations** to take full advantage of emerging opportunities*

If the number of orders drops below my daily/weekly estimate

Warning if the delivery of goods is lower than 80% of ready to ship.

If the ratio between web and phone orders are higher than ...

If the number of errors in incoming EDI messages is higher then 5% of total

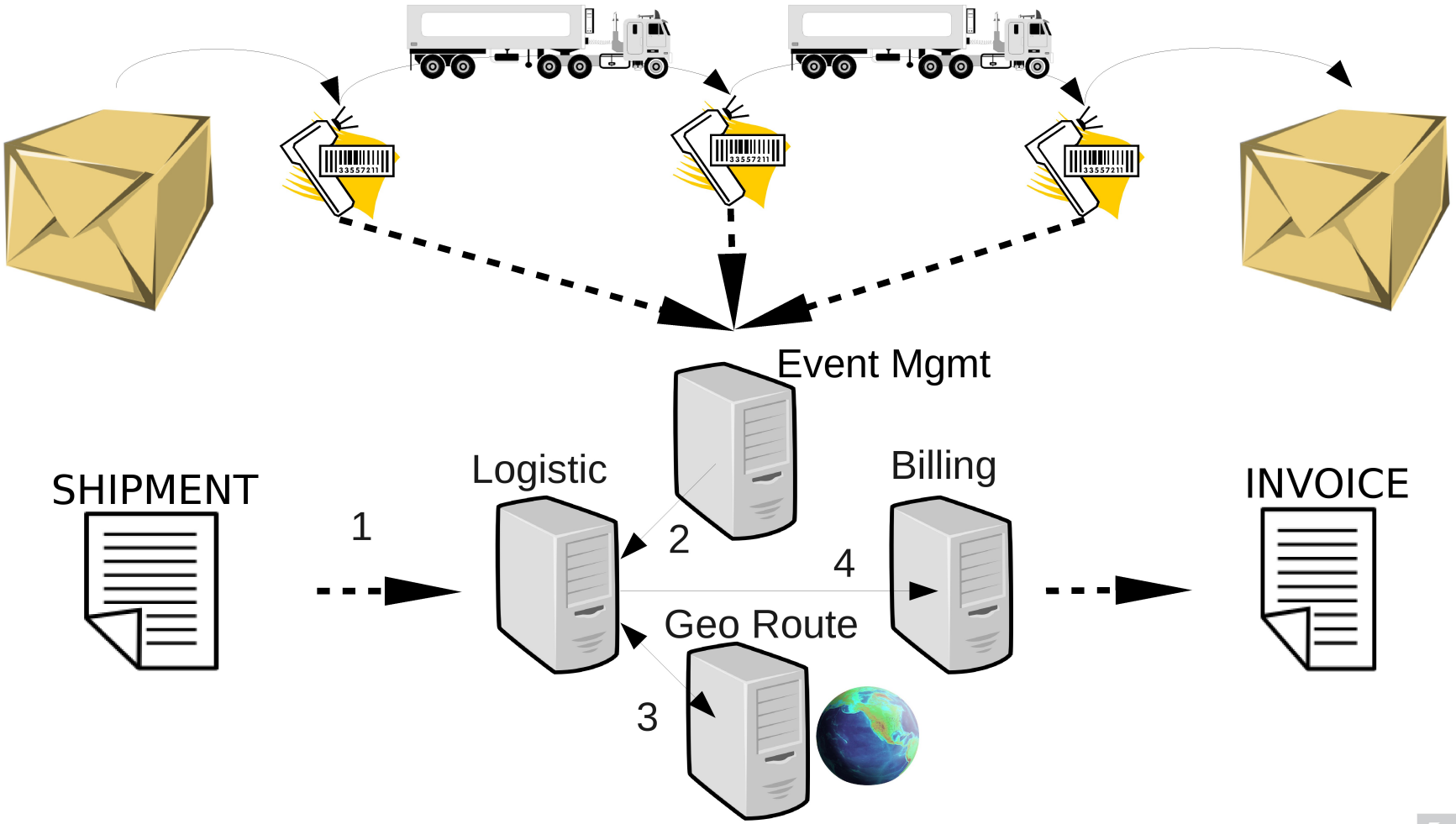
My route planning must be at least 90% of my received orders

If the number of international shipments is above 10000 at 17:00 I need to give the gateway terminal a warning

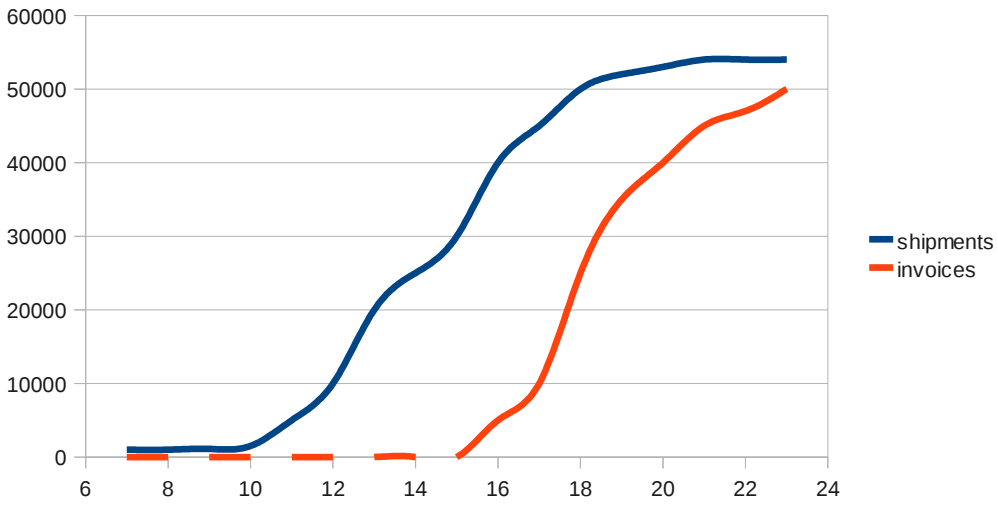
Findings

- Limited or no monitoring solutions
- When problems are detected it's to late to fix it them
- It's not an IT-OPS problem
- Not a BI issue - lack of real-time
- Low surveillance maturity in the business OPs
- Applications lack business surveillance interfaces
- SLA is of technical nature

Transportation example

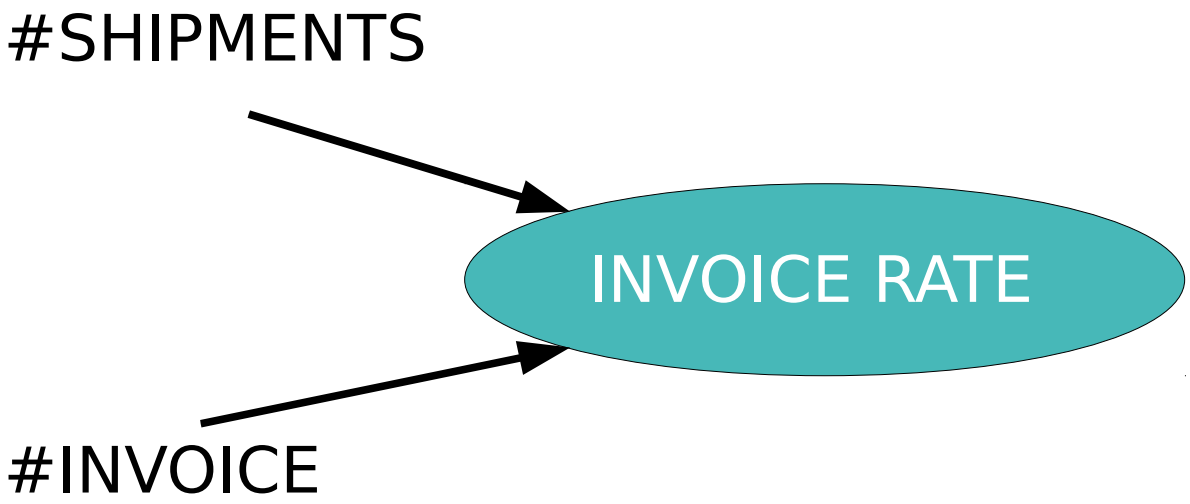


Metrics

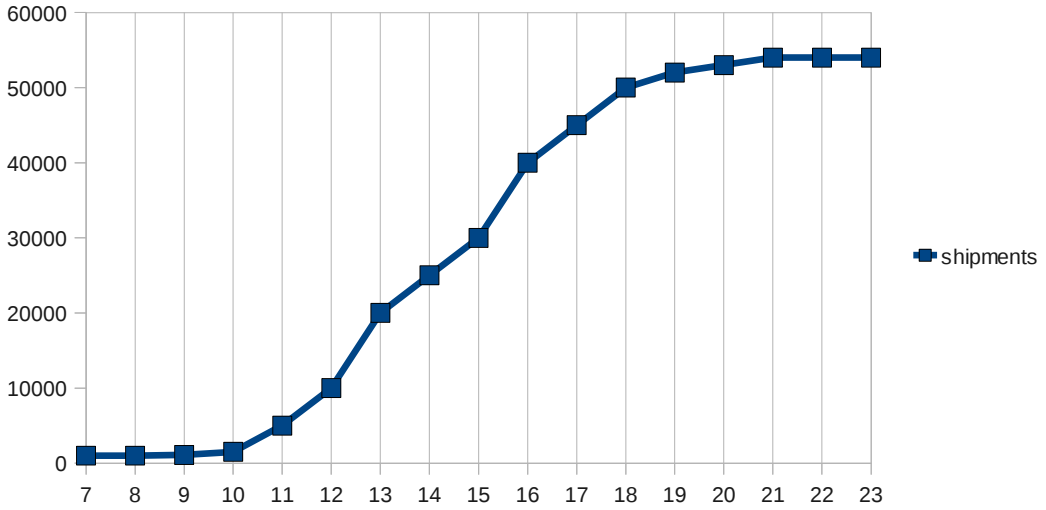


- Time
  - Day of week, day of month, ……
  - Calendar
- Process related

Composite metrics



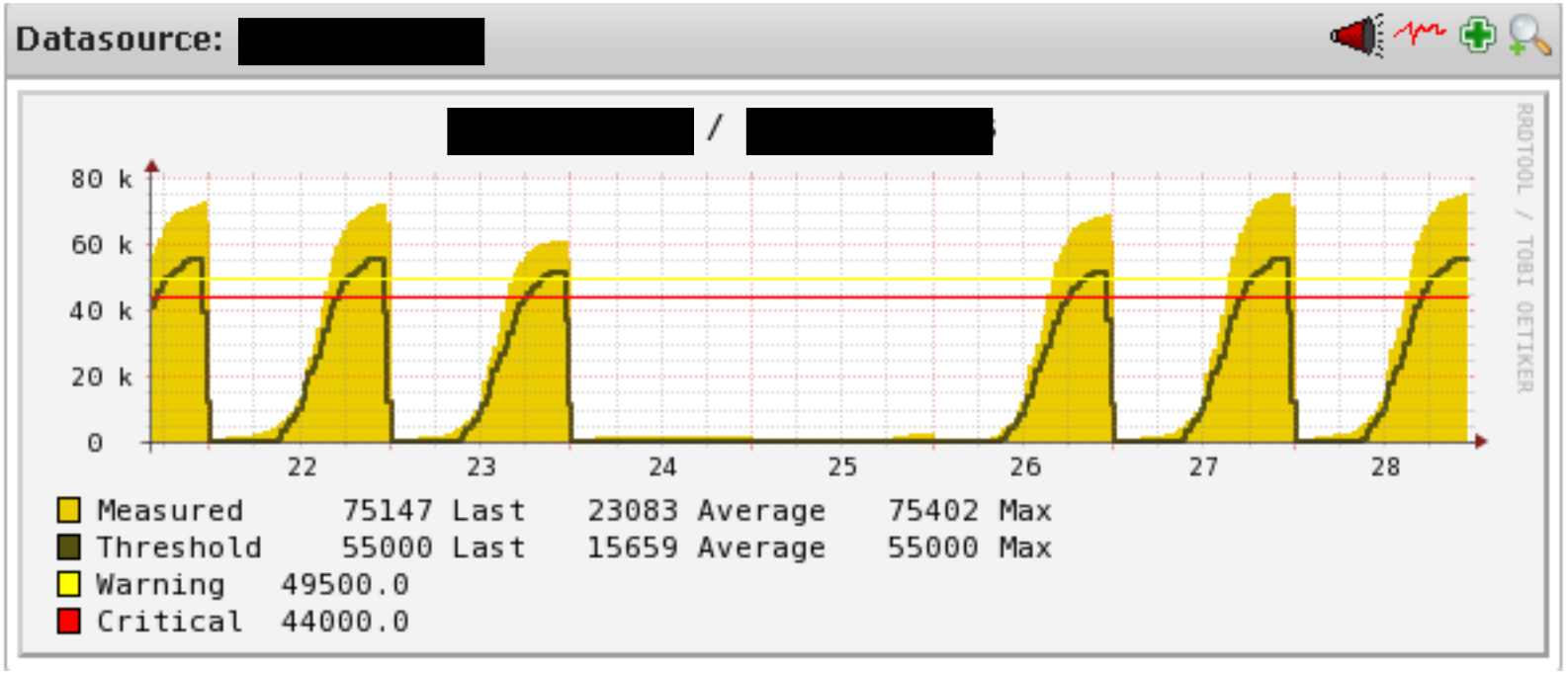
Process driven thresholds



- Day profiles
  - 24 hour granularity
  - Week, month, day of …
- Process related threshold
  - $threshold_{geocode} > \int (0.8*shipments)$
- Latency
  - $threshold_{geocode} > \int (0.8*shipments[-30min])$
- Composite
  - $threshold_{invoice\ errors} < \int ((shiperrors/shipments)*invoices)$

Nagios view

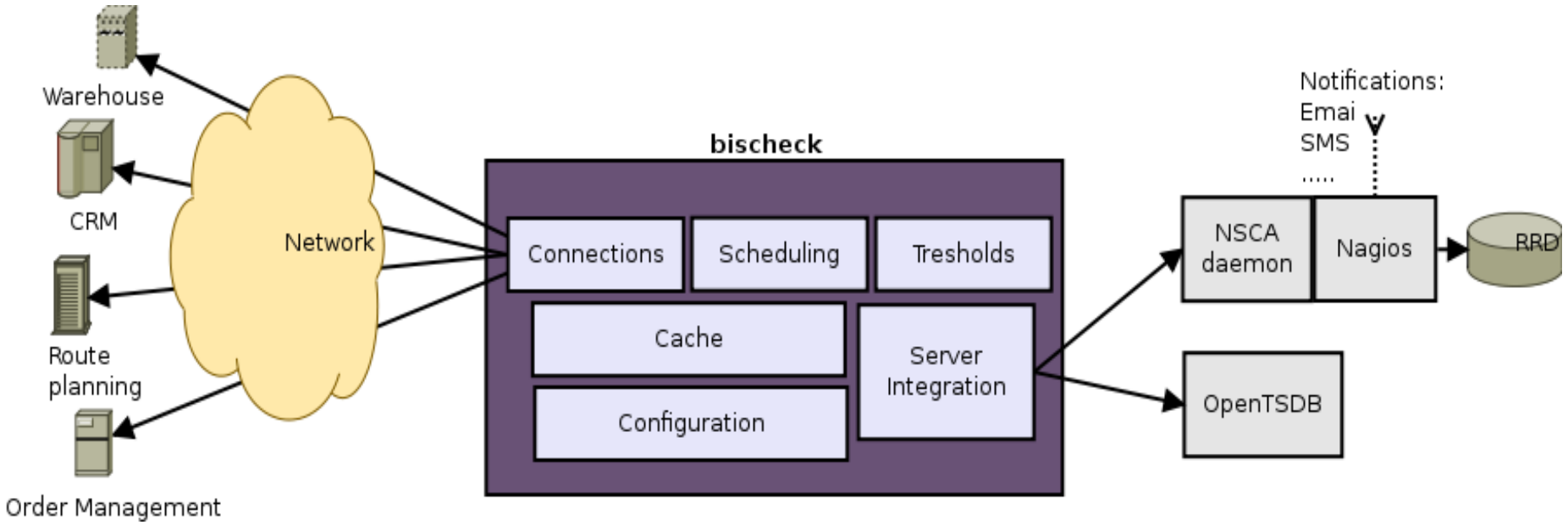
	[redacted]		2011-09-28 22:55:35	3d 21h 58m 53s	1/3	OK [redacted] = 75194 (55000.0 > 49500.0 > W > 44000.0 > C >)



Nature of BAM

- Operational
- Business events are **time dynamic** to it's nature
- Business events has **dependencies** to other events
- Service capability **relates** to multiple events

Solution – bischeck and Nagios



Bischeck features

- Service connections
- Dynamic threshold management
  - Packaged – a 24 hour linear equation threshold
  - Custom threshold classes
- Multi-threaded and multi-scheduling schema per service.
- Caching of historical service data
  - Virtual services
  - Latency threshold
- Date macros in execution statements
- Open server integration
  - Nagios/NSCA passive check
- XML configuration supported with WEBui
- GPL 2 license

Lack of BAM

- Simple problems cause disaster
  - High cost
  - Decreased quality of services
- Insecurity in business ops team
- Process correlation not understood
- IT resources utilization correlation to business operations

Get started with bischeck
and your favorite Nagios based distribution

Thank you for listening

- bischeck is open source - get it from **www.ingby.com** and **gforge.ingby.com/gf/project/bischeck**
- Feedback is appreciated