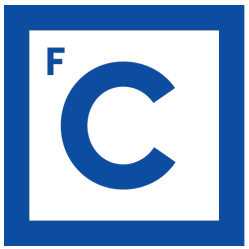
Monitoring

CGS - Hugo Miranda

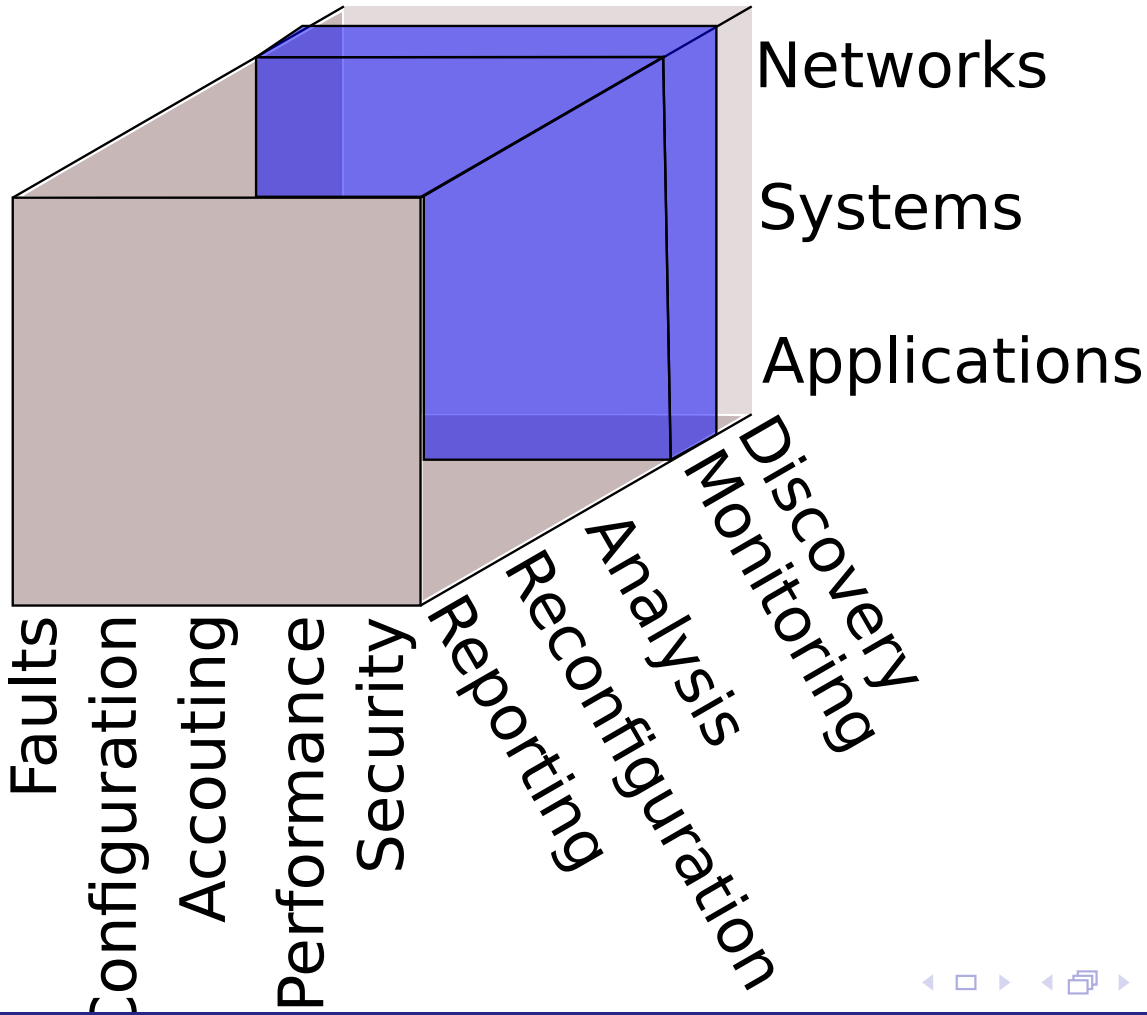
2021



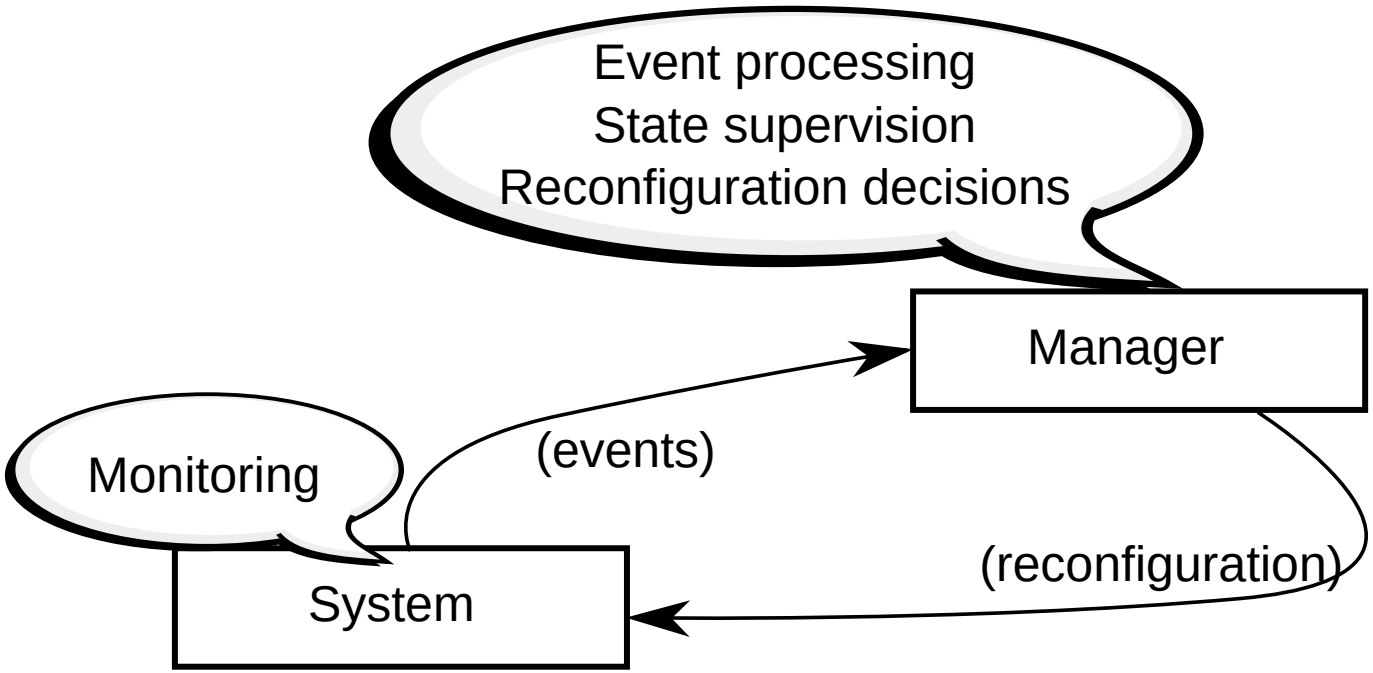
Ciências ULisboa

Faculdade de Ciências da Universidade de Lisboa

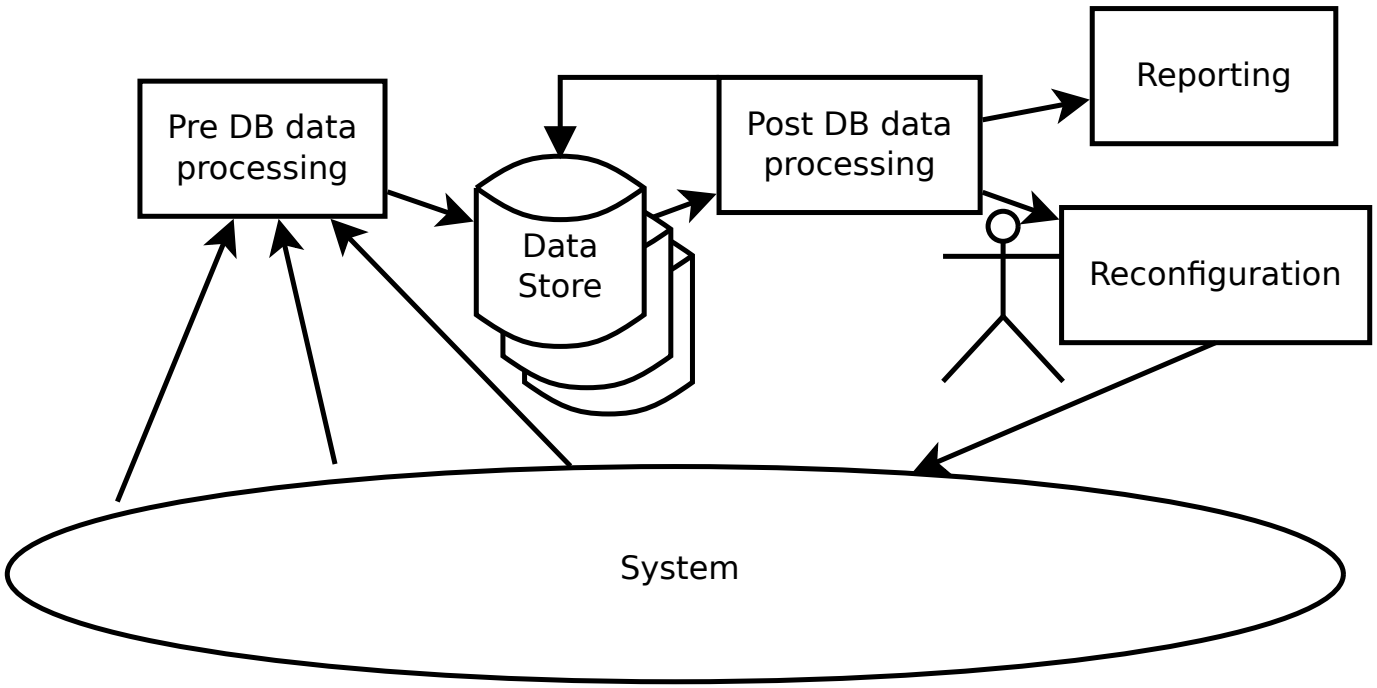
What to Monitor



The Big Picture



Data Flow


Pre DB data processing
Data Store
Post DB data processing
Reporting
Reconfiguration
System

Data Sources

Applications

- Logs
  - Count errors, accesses, etc.
- Proxies
  - Between the client and the server
- Fake requests
  - Withdraw/deposit money from a bank account
  - Request a web page
  - E.g. Site24x7 benchmark

Data Sources

Systems

- OS services
  - ps, who, uptime, free
- Logs
- Ping, IPMI, SNMP

Data Sources

Example (free)

```
$ free -h
              total        used        free      shared  buff/cache   available
Mem:           15Gi       1.6Gi       8.1Gi       162Mi       5.7Gi        13Gi
Swap:          19Gi          0B        19Gi

$ free | awk 'NR==2 {print $4;}'
```

Data Sources

Networks

- SNMP
  - traps/queries
- Fake nodes
  - Routing protocols
- Traffic observation
  - IPFIX
  - Port mirroring
- Diagnostic tools
  - Ping
  - Traceroute

Data Received

Status

- on/off/on with problems
- Ping
- Website responded

Configuration settings

- Certificate expire date
- DHCP lease range
- Number of threads for HTTP requests

Data Received

Statistics

- Free memory
- Number of 404 errors
- Response time
- Watermarks

Errors

Problems the agent is aware of

- Unexpected website response
- Route in cycle

How to cope with the large amount of data?

- Ask what you need to know
  - But not less than that

Passive Agents

Monitoring framework queries the agent

- Data flow regulated by monitoring framework
- Late discovery of problems
- Required to discover failed hardware/agent
- Requires 2 messages
- The authentication problem
  - Overhead for authenticating requester
  - Alternative is DoS vulnerability

Active Agent

Agent spontaneously notify the monitoring framework

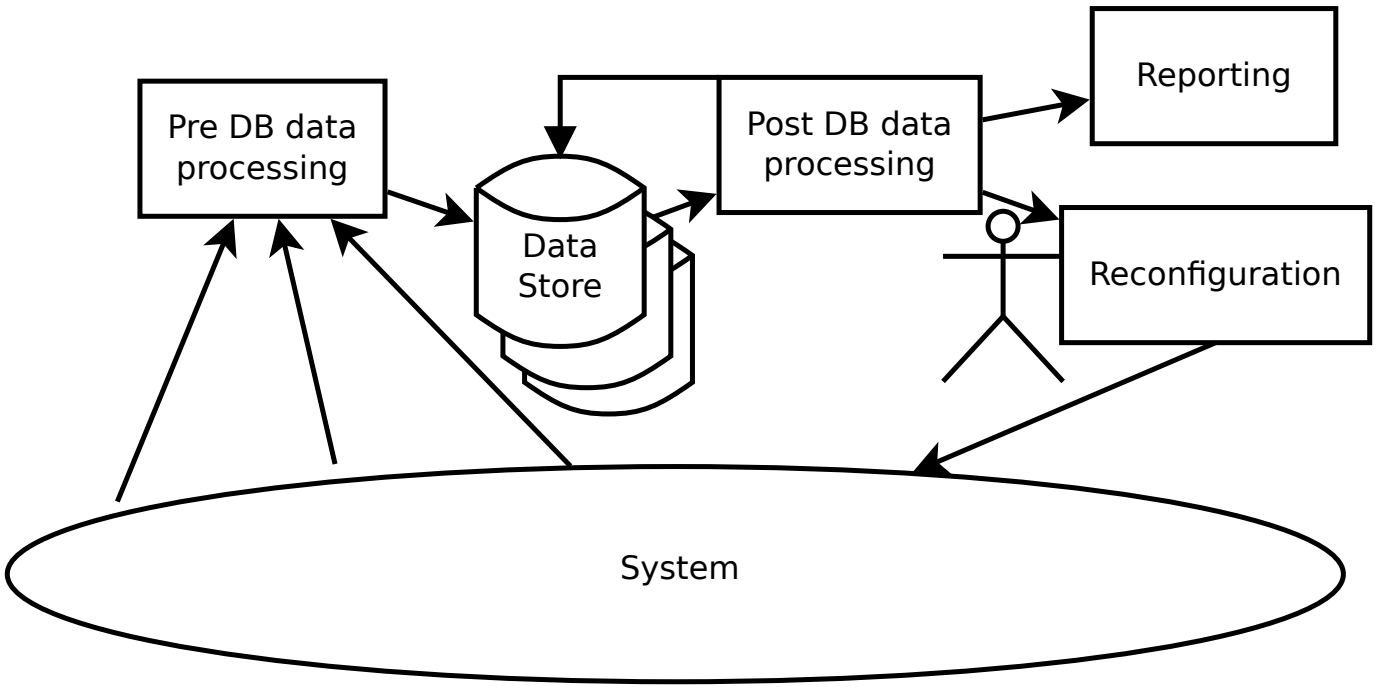
- E.g. SNMP traps
- Timely discovery of errors
- Can overload the monitoring framework
- Useless information/managed device resource consumption
- Risk of spontaneous synchronization
  - Random timers
  - Dynamic timers

Where to Calculate Metrics?

Performance problems may emerge when determining the metrics is computationally intensive

- On the managed entity
  - Impact on the managed entity performance
- Outside the managed entity
  - Requires the transfer of the file
- Write the file outside the managed entity
  - e.g. Elastic cloud/Kibana

Data Flow


Pre DB data processing
Data Store
Post DB data processing
Reporting
Reconfiguration
System

Why pre-processing?

- Data must make sense
- Errors can happen
- Facilitate storage and analysis

Partition data in tokens

- Depends of the agent and data
  - SNMP
  - Apache log files
- Tokens
  - Timestamp
  - Device ID
  - Metric
  - Value

Validate tokens and logic

- CPU utilization > 100%?
- Timestamp is in the past?
- Device ID exists?
- End date > start date?

Correct tokens and logic

What if data is wrong?

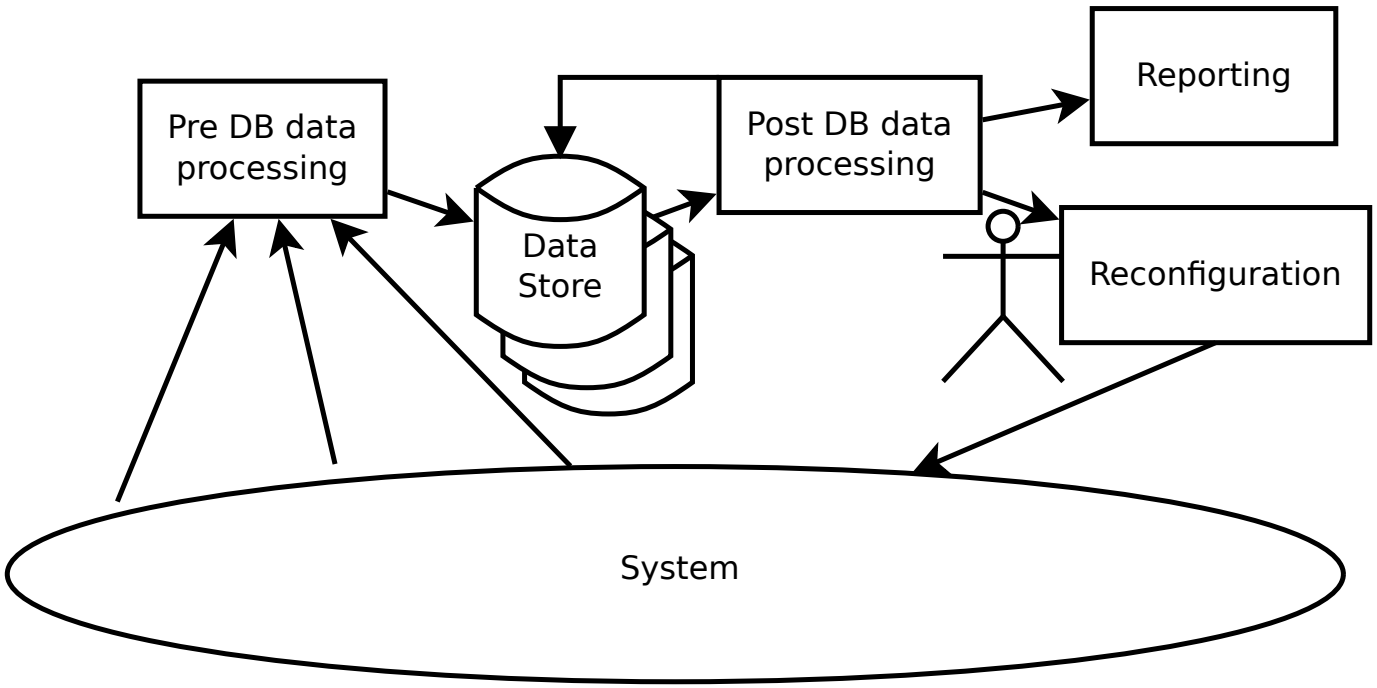
- Discard
  - Mark as unknown
- Recover
  - Repeat the last known value
    - Or weight the average of the n previous readings
  - Repeat the query
- Consider as a problem

Harmonize data

Make sure that comparable metrics are comparable

- Temperature in ºC
- Date format
- Power in W
- Time in ms

Data Flow


Pre DB data processing
Data Store
Post DB data processing
Reporting
Reconfiguration
System

Coping with Large Amounts of Data

- As the volume of data increases
  - so does time to query it
  - so does space required to store it
- More may not be better

Compress data

- Compress repetitions
  - *Up since Jan 5th 2016*
  - *Route unchanged since Feb 27th 2012*
- Thresholding
  - *Temperate lower than 60ºC except*
    - *Mar 3rd, 22h37m (65º),*
    - *Mar 4th, 15h18m (67º)*
- Discard replications
  - *Website served by 4 replicas. Average response time 750ms*

Degrade data

- Historical data is important but precision becomes irrelevant

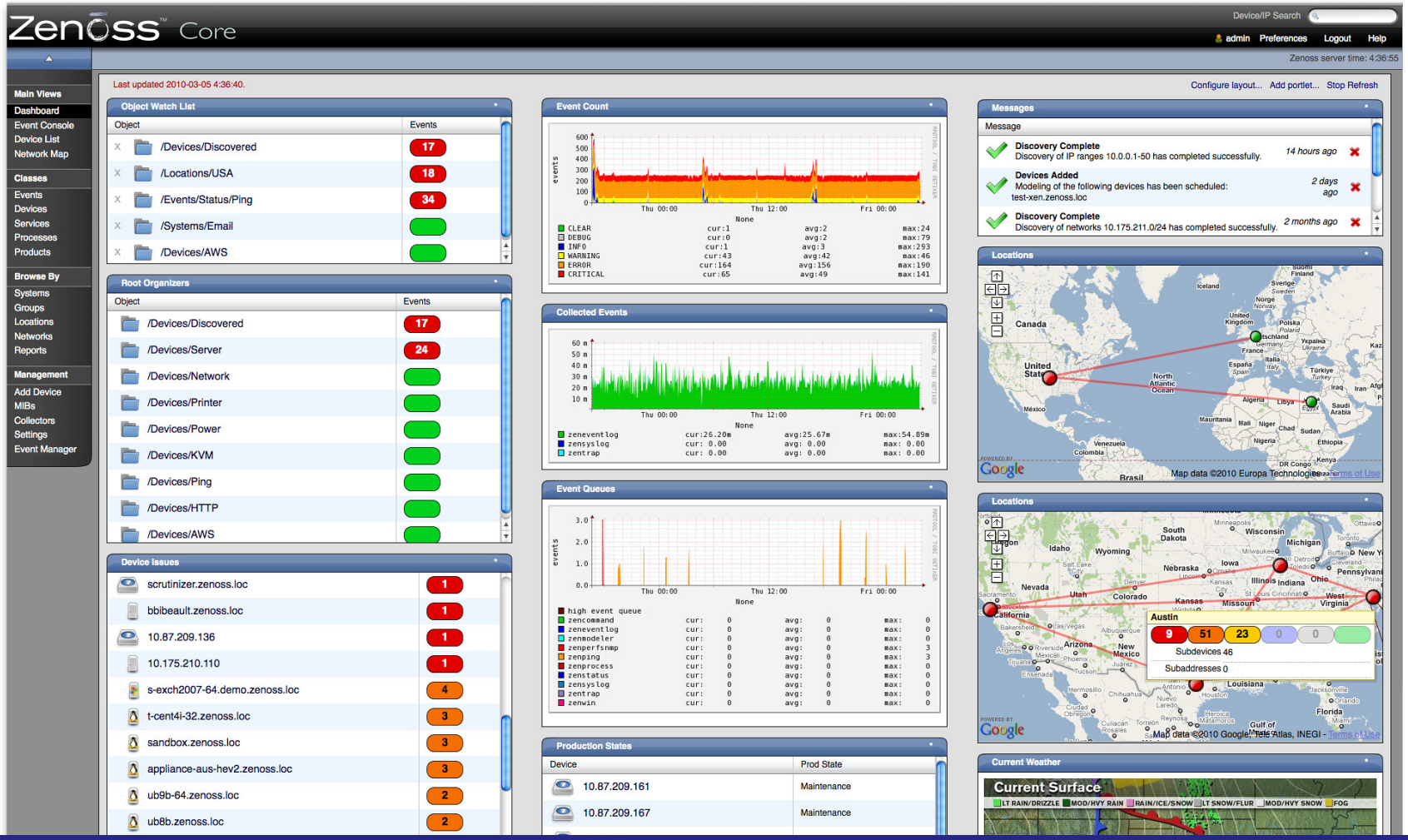
Interval	Data kept
Last 30 days	Every reading
30<t<60 days	Hourly max, min, average
60≤ t<180 days	Daily max, min, average
t≥180 days	Weekly max, min, average
	...

Data Store

Typical load balancing approaches for databases

- Distribute the data by several database instances
- Read-Only replication
- Round Robin Databases (RRD)
  - Circular buffers applied to databases
  - Works well with data degradation
- Hierarchical databases
  - Raw data is subsumed at multiple levels to facilitate analysis
- Rolling databases
  - Round robin at the database level

A Zenoss screenshot



Wrap Up

- Large amounts of data come in your way
  - Make sure that you get what you need
    - FCAPS (Not just Faults)
  - Make sure that you don't overwhelm the infrastructure to get what you don't need
- Keep cleaning
  - so that you can retrieve it when needed

What's Next

- Analysis, report and reconfiguration for FCAPS