Keeping an eye on your (IT) assets through Zabbix

Renante Yson

May 04, 2018

Department of Chemistry, University of Toronto

Introduction

The need for monitoring

- Resource planning
- Measure performance
- Ensure continuity
- Take control of assets
- Cut costs
- {...*many, many more*...}
- ... *But the most important of all*—Peace of mind

What monitoring systems can do

- Lookout for events and send alert when a problem is spotted
- Provide data when analyzing trends, e.g., spike in CPU usage during the off hours
- Provide data when analyzing network bandwidth — who is chewing up all the bandwidth?
- Aid in detecting network threats and other security issues

Our requirements

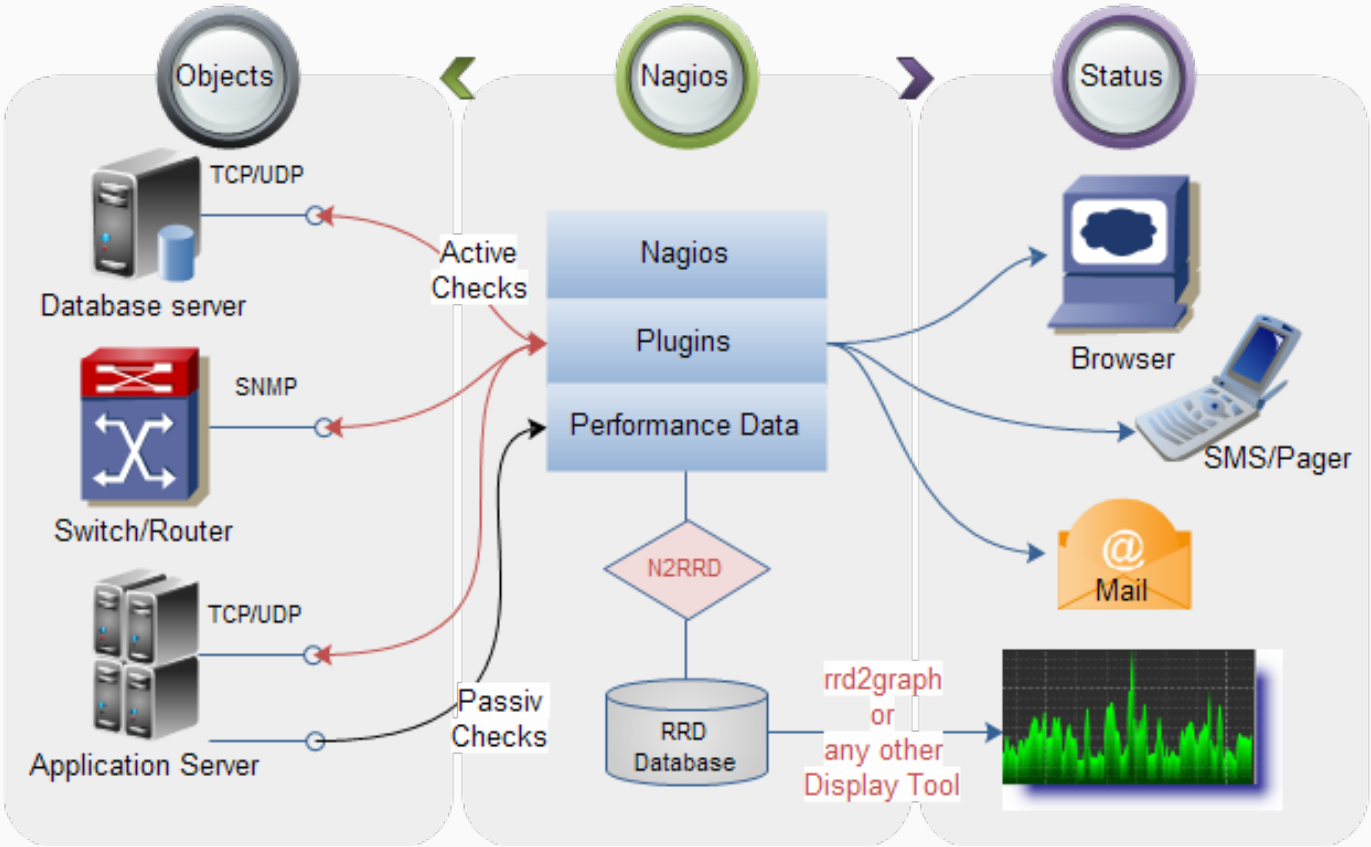
- Easy to install and learn
- Will be able to monitor from a variety of sources, methods, protocol
- Can be used for trend analysis
- Can be used with or without installing an agent
- Easy to use web interface

Nagios Core*

- First released in 1999
- Functions as an event monitoring and alerting engine
- File based/template configuration
- Supports active and passive checks, distributed monitoring and failover
- No builtin graphs but available through plugins/agents (nrpe, nrdp, etc)

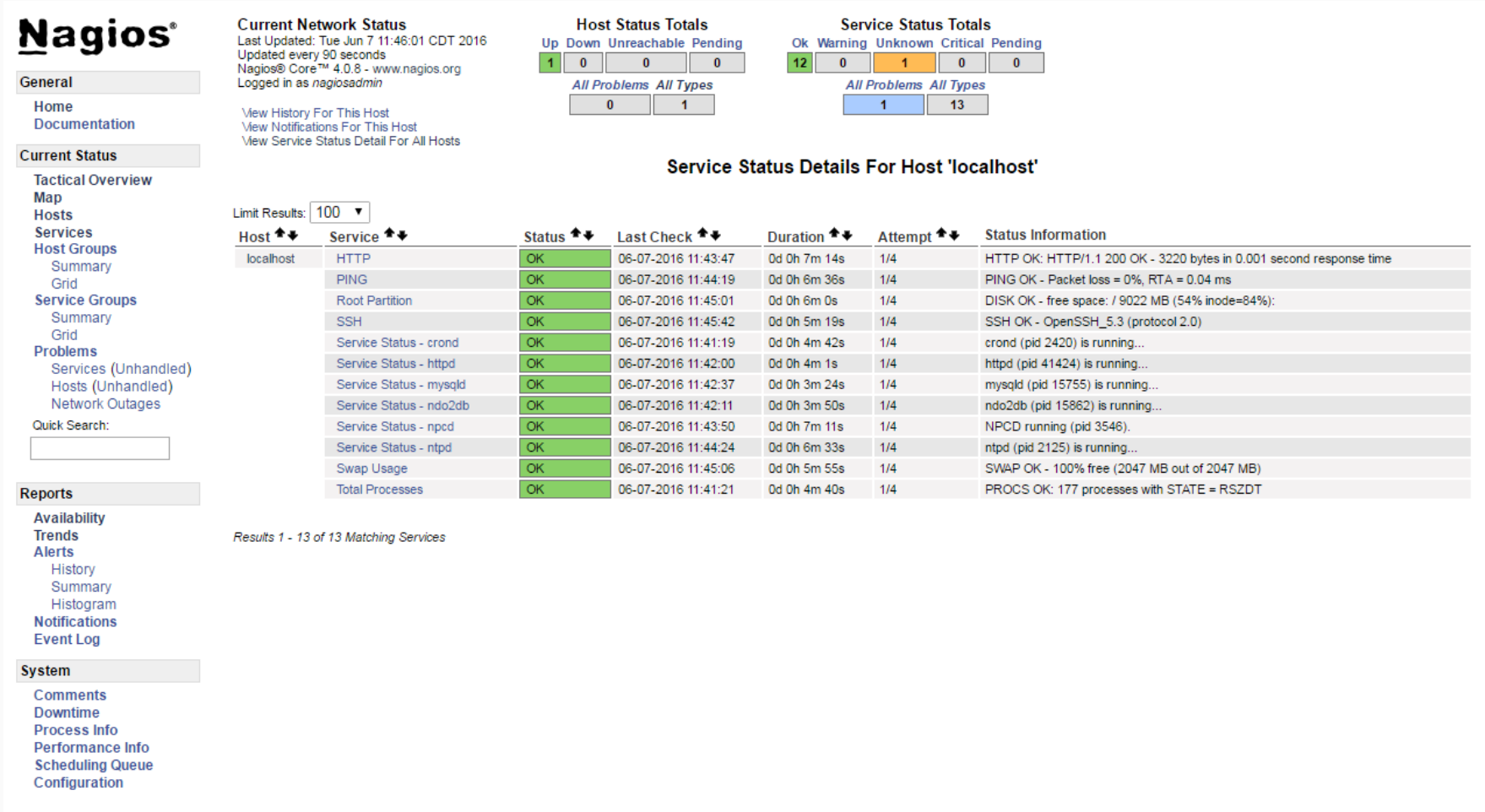
*`https://nagios.org`

Nagios Core operating principle



Source: `https://en.wikipedia.org/wiki/Nagios`

Nagios Core host monitoring



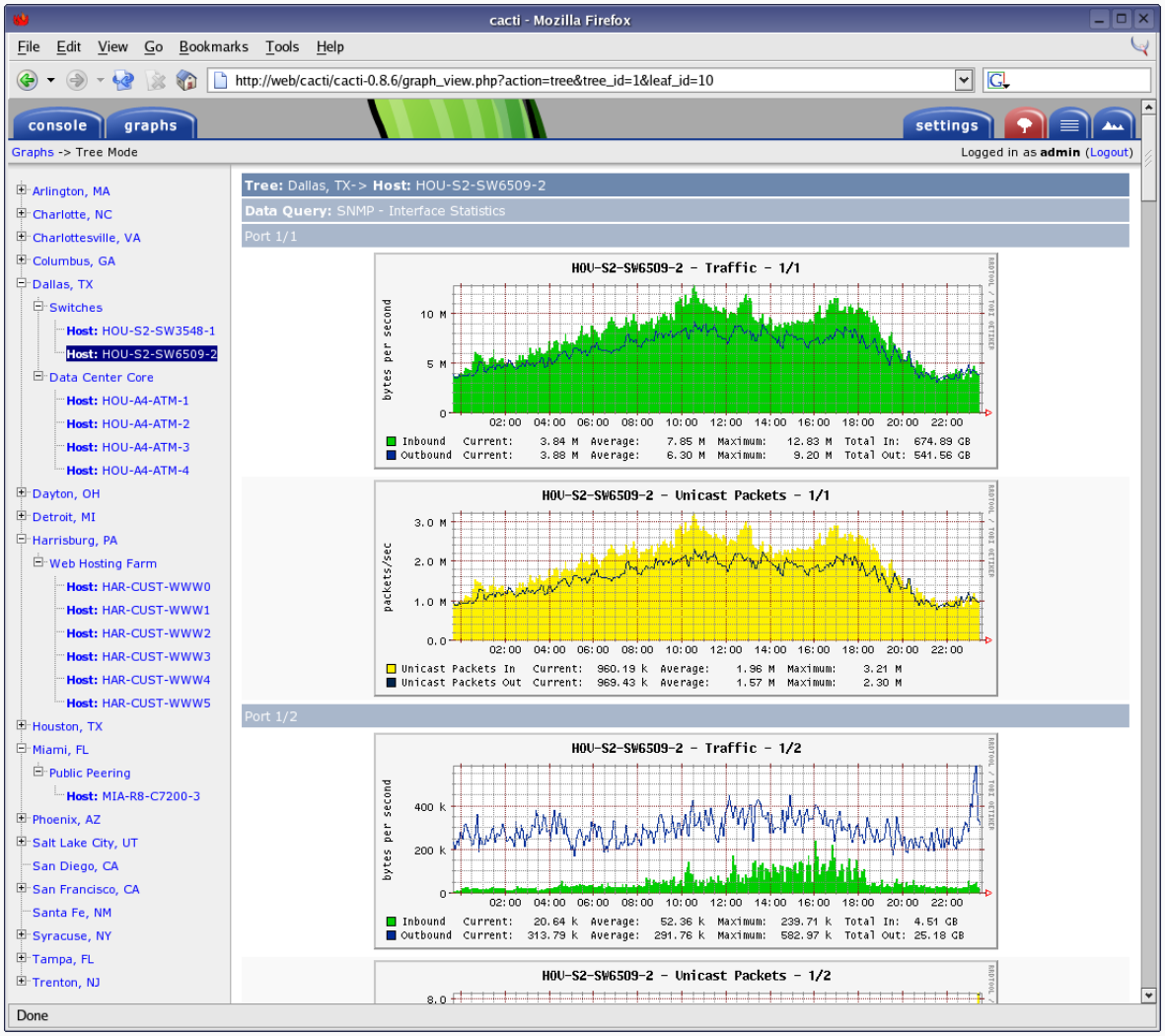
Source: `https://en.wikipedia.org/wiki/Nagios`

Cacti*

- Started in 2001
- A network monitoring and graphing tool
- Serves as a web frontend for RRDTool
- Great for trend analysis
- Gather data by SNMP
- Has built-in graphs and templates
- Other data sources can also be added by user

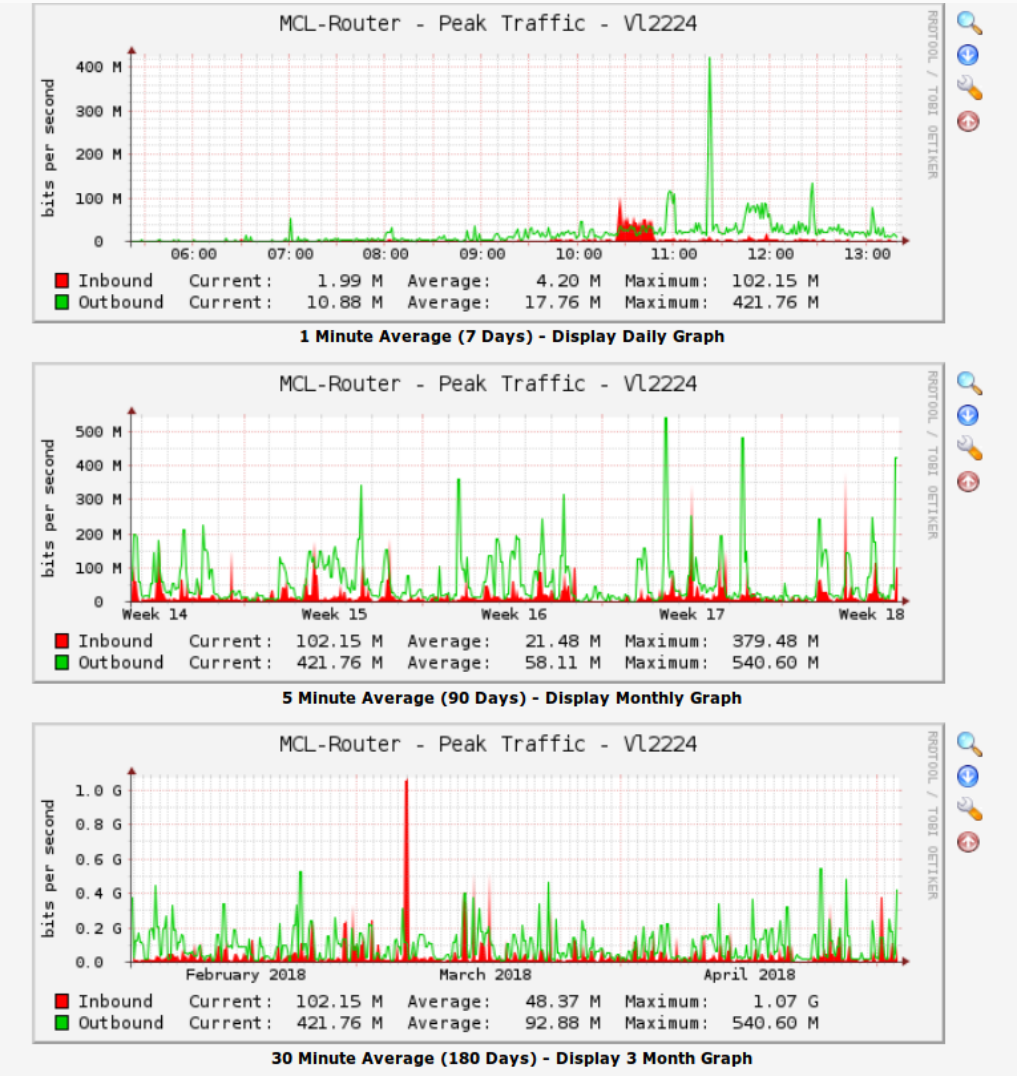
*https://cacti.net

Cacti graph



Source: `https://en.wikipedia.org/wiki/Cacti_(software)`

Cacti graph



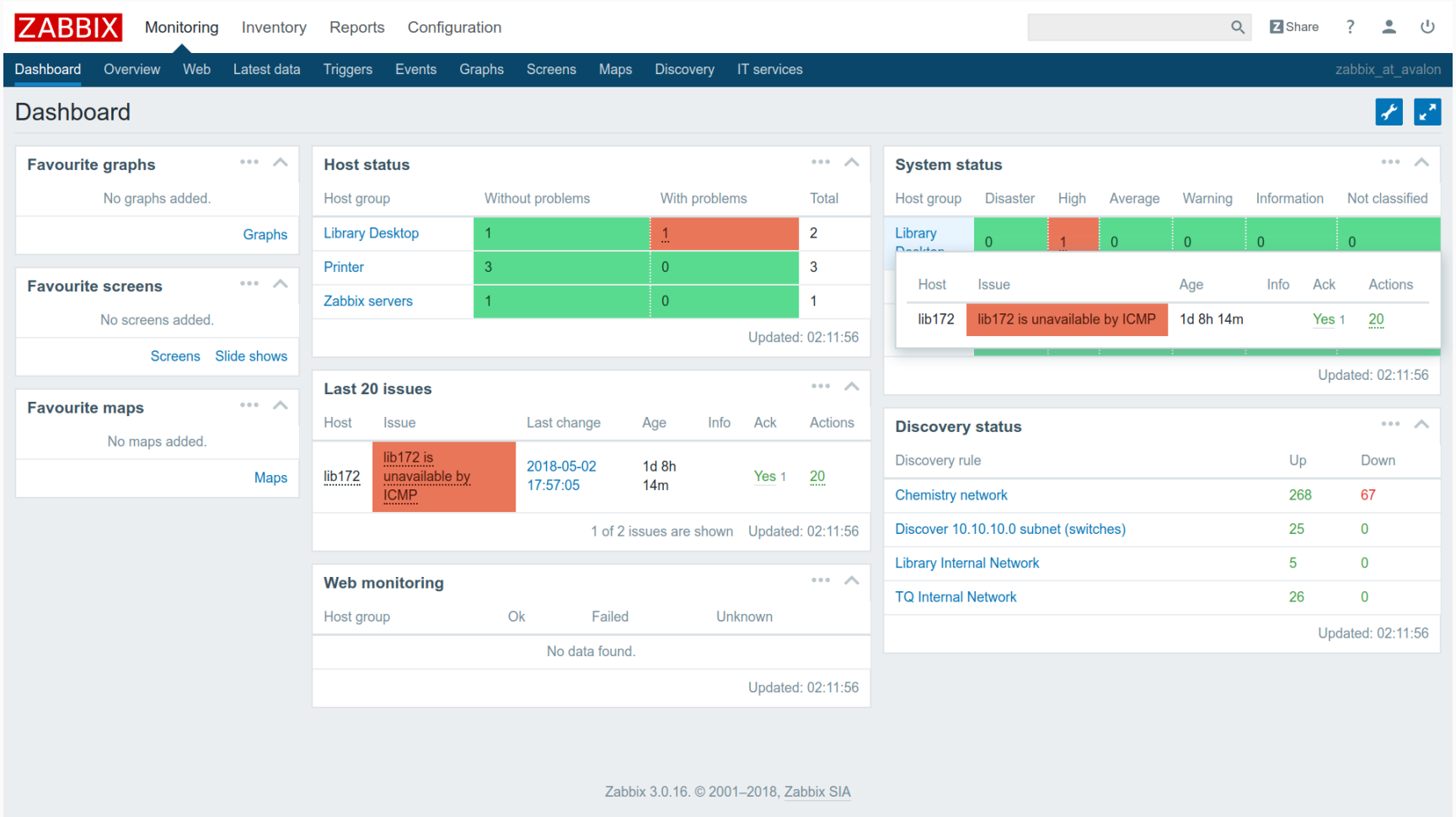
Source: `https://netmon.eis.utoronto.ca`

Zabbix*

- First stable release 2004
- Agentless monitoring of user services
- Active and passive check capability
- Distributed monitoring by proxy
- Multi-platform zabbix agent; both agent and proxy have small footprint
- Builtin SNMP and IPMI support
- Custom items
- Easy to install
- Builtin templates; also contributed at `https://share.zabbix.com/`

**https://zabbix.org*

Zabbix 3.0 dashboard



Google search trend

https://trends.google.com/trends/explore?date=today%205-y&q=zabbix,nagios,cacti,opennms,icinga

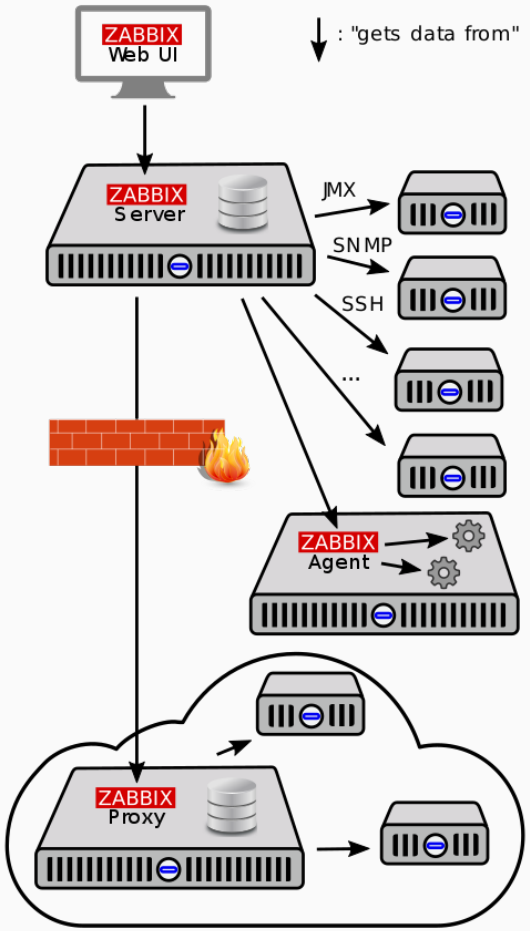
Zabbix

What is zabbix

Zabbix bills itself as *“the ultimate enterprise-level software designed for real-time monitoring of millions of metrics collected from tens of thousands of servers, virtual machines and network devices.”*

Zabbix is open source and comes at no cost.

Architecture



Source: `https://en.wikipedia.org/wiki/Zabbix`

Components

- Zabbix server: performs the polling and trapping of data, calculates triggers, sends notifications to users
- Database
- Web frontend
- Zabbix agent: deployed on target machines to actively monitor local resources and applications
- Zabbix proxy: collect monitoring data from one or more monitored devices and send the information to the Zabbix server

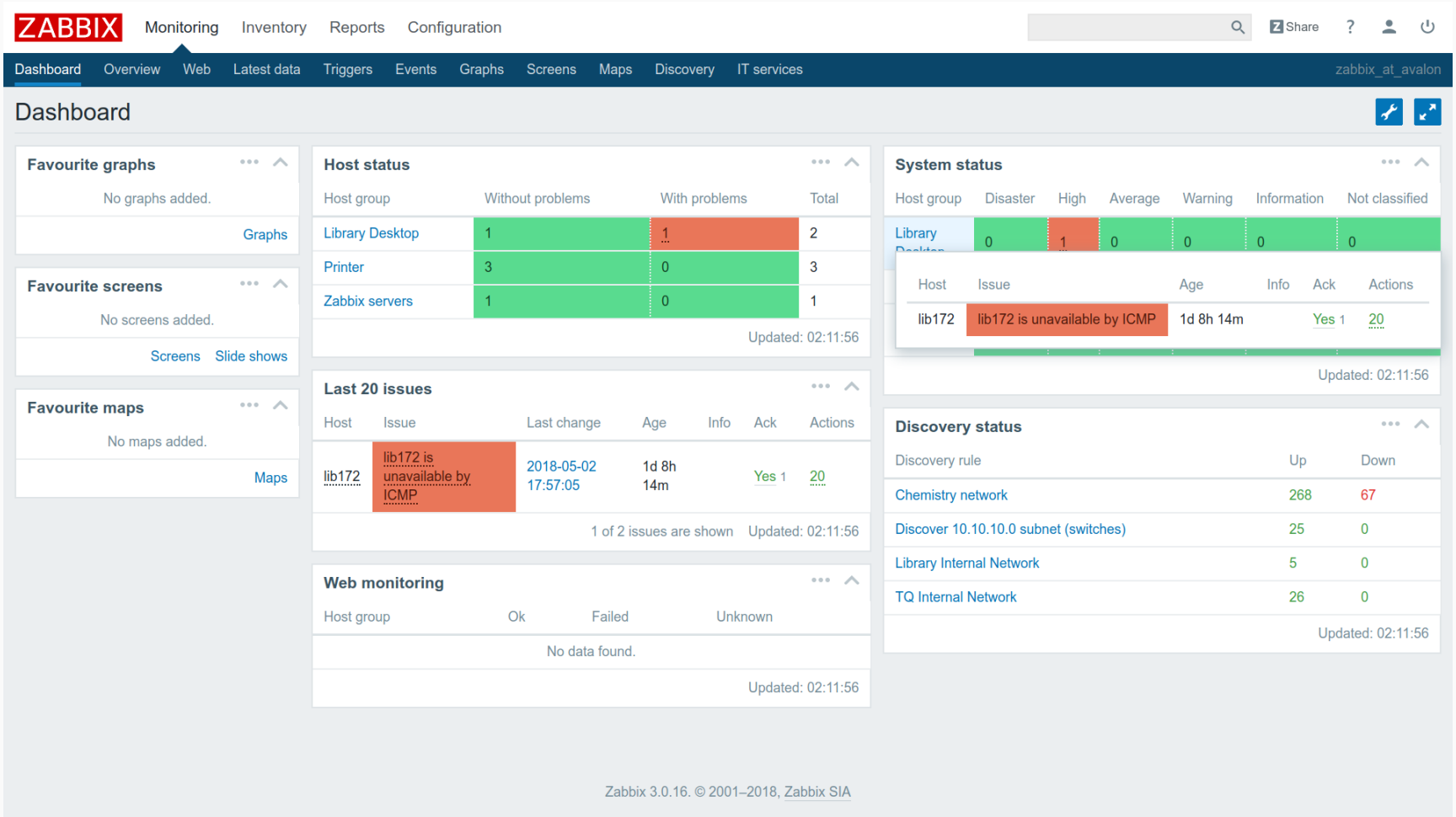
Items, hosts, host groups, templates

- item: a particular piece of data that you want to receive off of a host, a metric of data.
- host: a networked device that you want to monitor, with IP/DNS.
- host group: a logical grouping of hosts
- template: a set of entities (items, triggers, graphs, screens, applications, low-level discovery rules, web scenarios) ready to be applied to one or several hosts

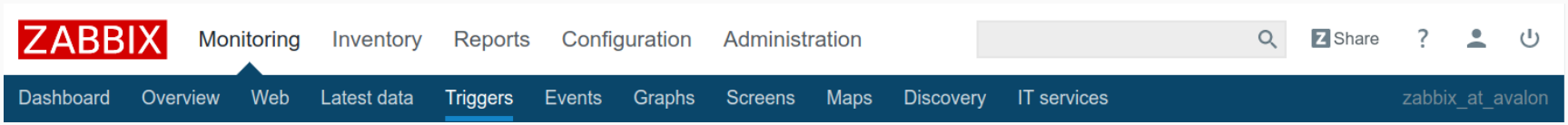
Some terms

- event: a single occurrence of something that deserves attention
- media: means of delivering notifications; delivery channel
- trigger: a logical expression that defines a problem threshold and is used to “evaluate” data received in items
- problem: a trigger that is in “Problem” state
- action: a predefined means of reacting to an event.
- escalation: a custom scenario for executing operations within an action; a sequence of sending notifications/executing remote commands

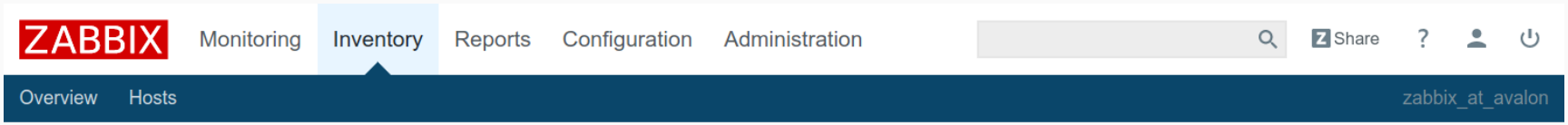
Zabbix 3.0 dashboard



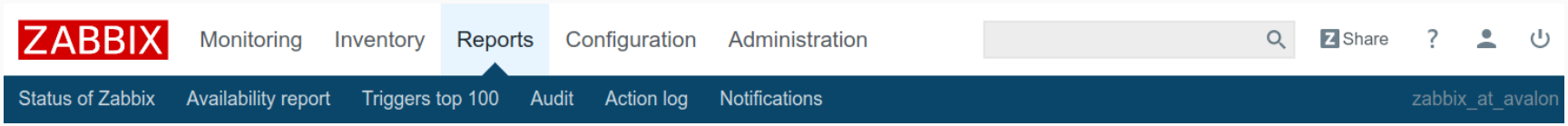
Monitoring menu



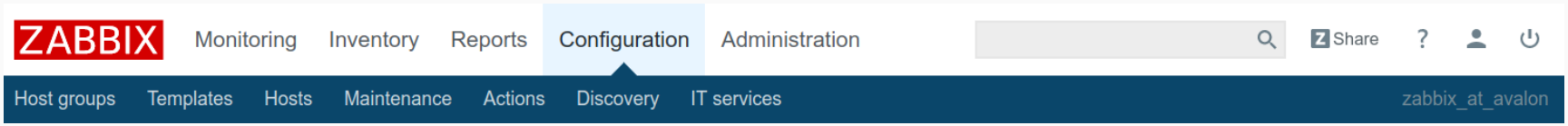
Inventory menu



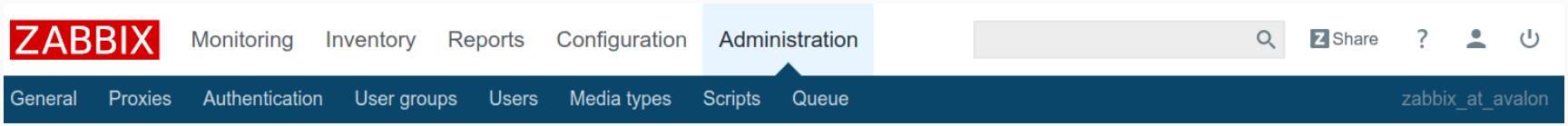
Report menu


ZABBIX
Monitoring
Inventory
Reports
Configuration
Administration
Share
Status of Zabbix
Availability report
Triggers top 100
Audit
Action log
Notifications
zabbix_at_avalon

Configuration menu



Administration menu



Problem alert example message

PROBLEM: Operational status was changed on interface GigabitEthernet1/0/7

@chem.utoronto.ca
Wed 4/25, 9:21 AM

Reply all

Trigger: Operational status was changed on interface GigabitEthernet1/0/7
Trigger status: PROBLEM
Trigger severity: Information
Trigger URL:

Item values:

1. Operational status of interface GigabitEthernet1/0/7 (:ifOperStatus[GigabitEthernet1/0/7]): down (2)
2. *UNKNOWN* (*UNKNOWN*:*UNKNOWN*): *UNKNOWN*
3. *UNKNOWN* (*UNKNOWN*:*UNKNOWN*): *UNKNOWN*

Original event ID: 261155

Resolution alert example message

RESOLVED: Status OK: CPU Load too high on for the last 3 minutes

@chem.utoronto.ca

Wed 5/2, 4:00 PM

Reply all

Trigger: CPU Load too high on for the last 3 minutes
Trigger status: OK
Trigger severity: Not classified
Trigger URL:

Item values:

1. CPU Load (:system.cpu.load): 0.57
2. *UNKNOWN* (*UNKNOWN*:*UNKNOWN*): *UNKNOWN*
3. *UNKNOWN* (*UNKNOWN*:*UNKNOWN*): *UNKNOWN*

Original event ID: 275301

What we monitor

- Services: mail server, webserver (apache, drupal, wordpress, DNS, NAT, etc.), MySQL databases, print server
- Computational clusters
- Virtual machines
- Windows servers
- Linux and windows desktops
- Managed network switches
- Printers: B/W HP Laserjets (SNMPv2c and v3), Multifunction printers/fax/scanner
- IPMI
- System logs

Our Implementation

Acknowledgments

ECF Team

- Dr. Violeta Gotcheva, Manager, Electronics and Computing Facility
- Jack Jackiewicz, Engineering Technologist
- Patrick Wong, Applications and Systems Software Programmer

Thank you!

References

- Zabbix: Enterprise Network Monitoring Made Easy by Rihards Olups, Andrea Dalle Vacche, and Patrik Uytterhoeven, *Packt Publishing Ltd.*, 2017.
- Zabbix v3.0 documentation, `https://www.zabbix.com/documentation/3.0/start`
- Zabbix: The enterprise class open source network monitoring solution, `https://www.zabbix.com`
- Wikipedia: Comparison of network monitoring systems, `https://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems`