

# 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

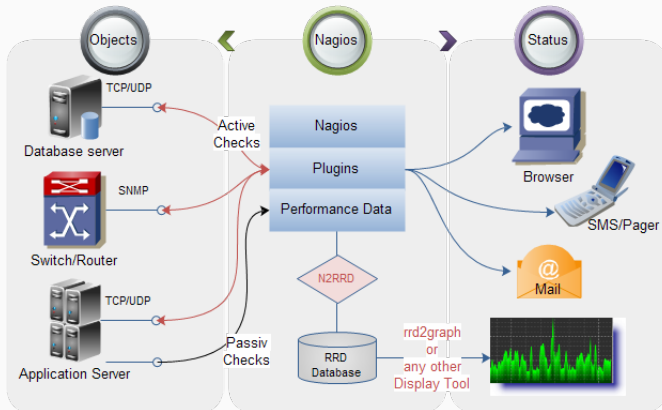
---

- 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

- 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

## Nagios®

### General

[Home](#)  
[Documentation](#)

### Current Status

[Tactical Overview](#)

[Map](#)

[Hosts](#)

[Services](#)

[Host Groups](#)

[Summary](#)

[Grid](#)

[Service Groups](#)

[Summary](#)

[Grid](#)

[Problems](#)

[Services \(Unhandled\)](#)

[Hosts \(Unhandled\)](#)

[Network Outages](#)

[Quick Search:](#)

### Reports

[Availability](#)

[Trends](#)

[Alerts](#)

[History](#)

[Summary](#)

[Histogram](#)

[Notifications](#)

[Event Log](#)

### System

[Comments](#)

[Downtime](#)

[Process Info](#)

[Performance Info](#)

[Scheduling Queue](#)

[Configuration](#)

### Current Network Status

Last Updated: Tue Jun 7 11:45:01 CDT 2016  
Updated every 90 seconds  
Nagios® Core™ 4.0.8 - www.nagios.org  
Logged in as nagiosadmin

[View History For This Host](#)  
[View Notifications For This Host](#)  
[View Service Status Detail For All Hosts](#)

### Host Status Totals

Up	Down	Unreachable	Pending
1	0	0	0
All Problems		All Types	
0		1	

### Service Status Totals

Ok	Warning	Unknown	Critical	Pending
12	0	1	0	0
All Problems		All Types		
1		13		

### Service Status Details For Host 'localhost'

Limit Results:

Host ♦♦	Service ♦♦	Status ♦♦	Last Check ♦♦	Duration ♦♦	Attempt ♦♦	Status Information
localhost	HTTP	OK	06-07-2016 11:43:47	0d 0h 7m 14s	1/4	HTTP OK: HTTP/1.1 200 OK - 3220 bytes in 0.001 second response time
	PING	OK	06-07-2016 11:44:19	0d 0h 6m 36s	1/4	PING OK - Packet loss = 0%, RTA = 0.04 ms
	Root Partition	OK	06-07-2016 11:45:01	0d 0h 6m 0s	1/4	DISK OK - free space: / 9022 MB (54% inode=84%):
	SSH	OK	06-07-2016 11:45:42	0d 0h 5m 19s	1/4	SSH OK - OpenSSH_5.3 (protocol 2.0)
	Service Status - crond	OK	06-07-2016 11:41:19	0d 0h 4m 42s	1/4	crond (pid 2420) is running...
	Service Status - httpd	OK	06-07-2016 11:42:00	0d 0h 4m 1s	1/4	httpd (pid 41424) is running...
	Service Status - mysqld	OK	06-07-2016 11:42:37	0d 0h 3m 24s	1/4	mysqld (pid 15755) is running...
	Service Status - ndo2db	OK	06-07-2016 11:42:11	0d 0h 3m 50s	1/4	ndo2db (pid 15862) is running...
	Service Status - npcd	OK	06-07-2016 11:43:50	0d 0h 7m 11s	1/4	NPCD running (pid 3546).
	Service Status - ntpd	OK	06-07-2016 11:44:24	0d 0h 6m 33s	1/4	ntpd (pid 2125) is running...
	Swap Usage	OK	06-07-2016 11:45:06	0d 0h 5m 55s	1/4	SWAP OK - 100% free (2047 MB out of 2047 MB)
	Total Processes	OK	06-07-2016 11:41:21	0d 0h 4m 40s	1/4	PROCS OK: 177 processes with STATE = RSZDT

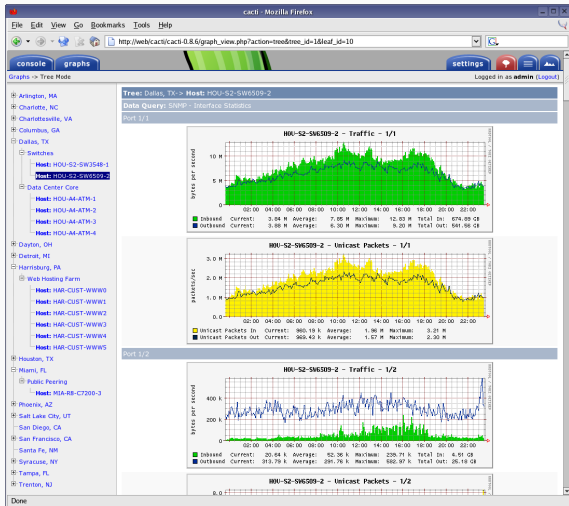
Results 1 - 13 of 13 Matching Services



- 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

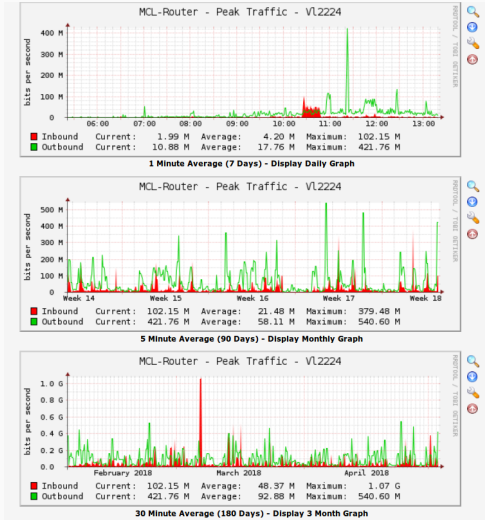
\*<https://cacti.net>

# CACTI GRAPH



Source: [https://en.wikipedia.org/wiki/Cacti\\_\(software\)](https://en.wikipedia.org/wiki/Cacti_(software))

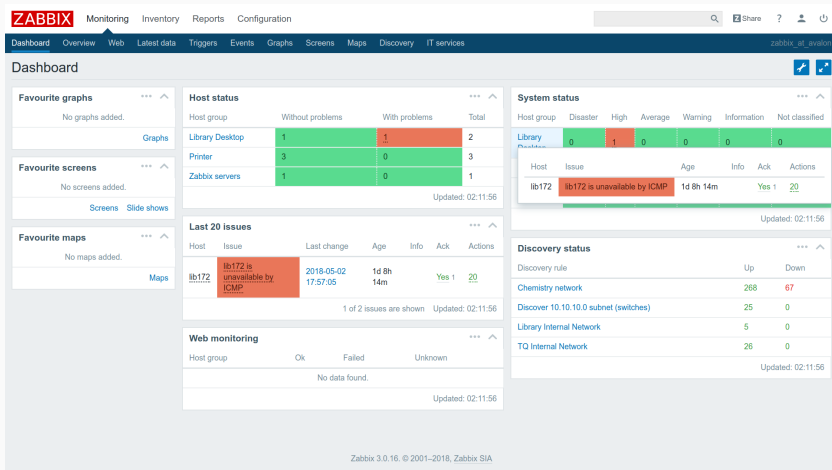
# CACTI GRAPH



- 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
```

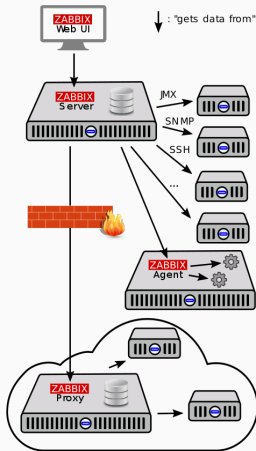
Zabbix

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

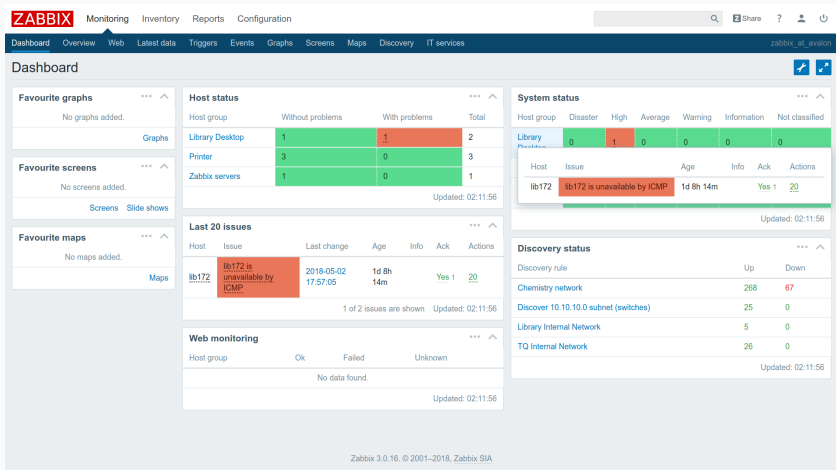
- **item**: a particular piece of data that you want to receive off of a host, a metric of data.
- **host**: a networked device that you want to monitor, with IP/DNS.
- **host group**: a logical grouping of hosts
- **template**: a set of entities (items, triggers, graphs, screens, applications, low-level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

## SOME TERMS

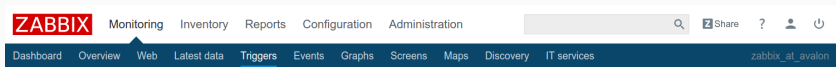
---

- **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

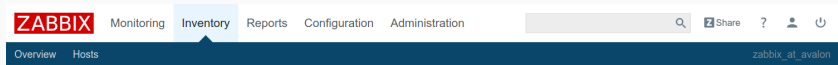
# ZABBIX 3.0 DASHBOARD



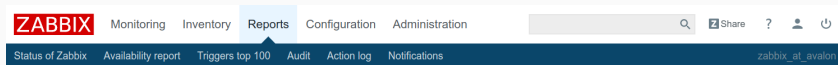
## Monitoring menu



## Inventory menu

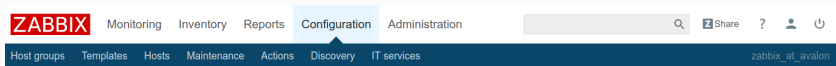


## Report menu

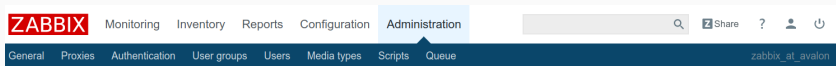




## Configuration menu



## 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 | v

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 `ibmcloud` for the last 3 minutes



@chem.utoronto.ca

Wed 5/2, 4:00 PM



Reply all | v

Trigger: CPU Load too high on `ibmcloud` for the last 3 minutes

Trigger status: OK

Trigger severity: Not classified

Trigger URL:

Item values:

1. CPU Load (`ibmcloud: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

## 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](https://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems)