



Services

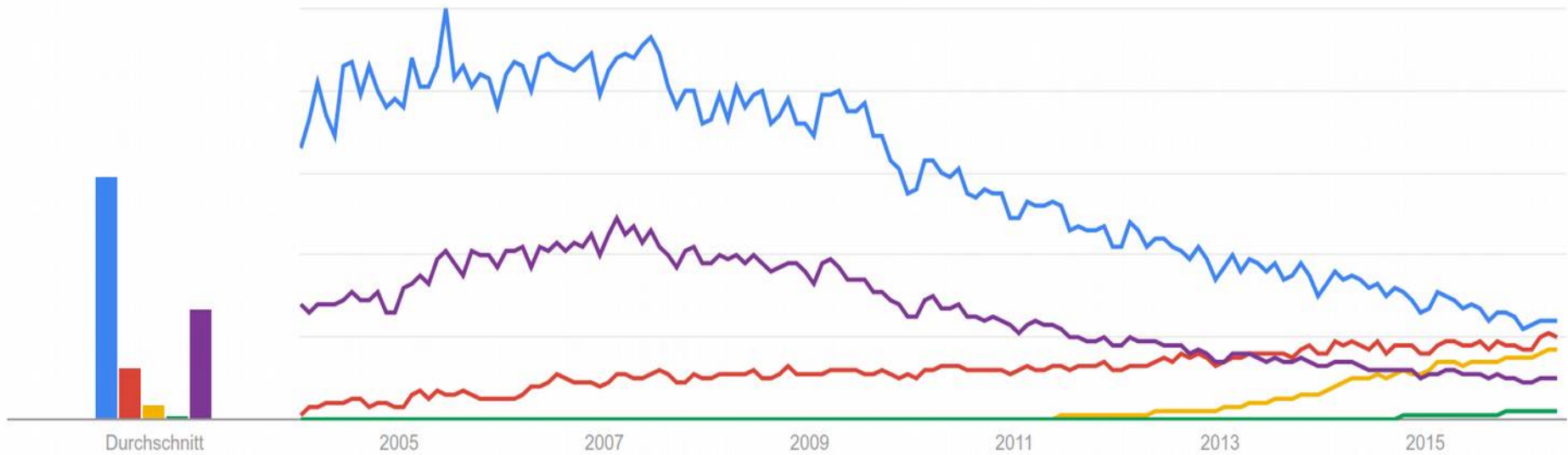
Bits & Bytes

Infrastructure Monitoring using Zabbix

Contact

Thanks to

UnFUCK.eu – Unix Friends and User Campus





- GUI walk-through
- Zabbix architecture
- Zabbix agent
- High-Availability
- Release 3.0 & Upcoming
- Monitoring & Analytics
- Q & A



• Monitoring → Dashboard

ZABBIX Monitoring Inventory Reports Configuration Administration

Dashboard Overview Web Latest data Triggers Events Graphs Screens Maps Discovery IT services

Dashboard

Favourite maps

- Local network

Favourite graphs

- New host: CPU load

Favourite screens

- Zabbix server

Last 20 issues

| HOST | ISSUE | LAST CHANGE | AGE | INFO | ACK | ACTIONS |
|-----------------|---|---------------------|--------|------|-------|-------------------|
| Zabbix server 1 | Version of zabbix-agent(d) was changed on Zabbix server 1 | 2016-01-11 22:36:06 | 1m 39s | | No | 1 |
| Zabbix server 1 | Lack of free swap space on Zabbix server 1 | 2015-08-11 23:29:28 | 5m 3d | | Yes 4 | |

2 of 2 issues are shown Updated: 22:37:45

System status

| HOST GROUP | DISASTER | HIGH | AVERAGE | WARNING | INFORMATION | NOT CLASSIFIED |
|------------------|----------|------|---------|-------------------|-------------------|----------------|
| Discovered hosts | 0 | 0 | 0 | 1 | 1 | 0 |
| Network devices | 0 | 0 | 0 | 0 | 0 | 0 |
| SNMP hosts | 0 | 0 | 0 | 0 | 0 | 0 |
| Zabbix servers | 0 | 0 | 0 | 1 | 1 | 0 |

Updated: 22:37:45

Host status

| HOST GROUP | WITHOUT PROBLEMS | WITH PROBLEMS | TOTAL |
|------------------|------------------|-------------------|-------|
| Discovered hosts | 7 | 1 | 8 |
| Network devices | 1 | 0 | 1 |
| SNMP hosts | 2 | 0 | 2 |
| Zabbix servers | 0 | 1 | 1 |

Updated: 22:37:44

Discovery status

| DISCOVERY RULE | UP | DOWN |
|----------------|----|-------------------|
| Local network2 | 6 | 1 |

Updated: 22:37:44

Status of Zabbix

| PARAMETER | VALUE | DETAILS |
|--|-------|-----------------|
| Zabbix server is running | Yes | localhost:10051 |
| Number of hosts (enabled/disabled/templates) | 54 | 10 / 1 / 43 |
| Number of items (enabled/disabled/not supported) | 356 | 350 / 0 / 6 |
| Number of triggers (enabled/disabled [problem/ok]) | 95 | 94 / 1 [2 / 92] |
| Number of users (online) | 3 | 2 |
| Required server performance, new values per second | 4.79 | |

Updated: 22:37:45

Web monitoring

| HOST GROUP | OK | FAILED | UNKNOWN |
|------------------|----|--------|---------|
| Discovered hosts | 1 | 0 | 0 |
| Zabbix servers | 1 | 0 | 0 |

Updated: 22:37:44

[Debug](#)



- **Search**
 - Search for a host, template and host group configuration
- **Zabbix Share (share.zabbix.com)**
- **Help (zabbix.com/documentation/3.0/)**
- **User Profile Settings**

- **Monitoring**
 - **Dashboard Setting**
 - **Dashboard**
 - Status of the Zabbix server, number of hosts, items, triggers, vps (values per second)
 - System status: Systems has any problem?: yes or no
 - Host status: Detailed status by severity
 - Latest issues: By default it only shows last 20 issues. This value can be changed. If you want to see all triggers, then use “Monitoring → Overview” or “Monitoring → Triggers”.
 - Graphs, screens, maps



- **Monitoring** → **Overview**

- Filter monitoring metrics by application. Zabbix allows you very easy to assign monitoring metrics to an application. E.g. metrics of application “IMCP”: ICMP loss, ICMP response time, ICMP ping.
- Filter Triggers
 - The Dashboard only shows last 20 issues by default. Here you can filter everything related to triggers (e.g. by severity, acknowledged or not)

The screenshot shows the Zabbix Overview page. At the top, there are filters for Group (all), Type (Data), and Hosts location (Top). Below this is a 'Filter' section with a dropdown menu set to 'Performance' and a 'Select' button. There are also 'Filter' and 'Reset' buttons. The main content is a table with the following data:


| ITEMS | NEW HOST | ZABBIX SERVER |
|--|-----------|---------------|
| Context switches per second | 4.55 Ksps | 169 sps |
| CPU idle time | 0 % | 86.72 % |
| CPU interrupt time | 0 % | 0 % |
| CPU iowait time | 0 % | 1.02 % |
| CPU nice time | 0.0083 % | 0 % |
| CPU softirq time | 0.02 % | 0.26 % |
| CPU steal time | 0 % | 0 % |
| CPU system time | 85 % | 4.4 % |
| CPU user time | 15.22 % | 7.15 % |
| Interrupts per second | 3.3 Kips | 74 ips |
| Processor load (1 min average per core) | 2.38 | 0.03 |
| Processor load (5 min average per core) | 1.79 | 0.06 |
| Processor load (15 min average per core) | 1.07 | 0.06 |



- **Monitoring** → **Web**
 - See status of agentless checks, which are executed directly from the Zabbix server
 - Filter such metrics by hostgroups or hosts



- **Monitoring** → **Latest data**
 - Fine grained metric filtering (by host group and hosts, as well as by application-, metric- or trigger name)
 - Triggers:
 - Fined grained trigger filtering, very similar to “Overview” → “Trigger”

Latest data 

Filter ▲

Host groups Name

Hosts Show items without data

Application Show details

| <input type="checkbox"/> | HOST | NAME ▼ | LAST CHECK | LAST VALUE | CHANGE | |
|-------------------------------------|---------------|------------------------------------|---------------------|------------|--------------|-----------------------|
| ▼ | Zabbix server | Network interfaces (2 Items) | | | | |
| <input type="checkbox"/> | | Outgoing network traffic on enp0s3 | 2016-01-02 20:24:07 | 31.78 Kbps | -31.35 Kbps | Graph |
| <input checked="" type="checkbox"/> | | Incoming network traffic on enp0s3 | 2016-01-02 20:24:06 | 6.03 Kbps | -2.29 Kbps | Graph |
| ▼ | New host | Network interfaces (2 Items) | | | | |
| <input type="checkbox"/> | | Outgoing network traffic on eth0 | 2016-01-02 20:24:05 | 2.12 Kbps | -14.12 Kbps | Graph |
| <input checked="" type="checkbox"/> | | Incoming network traffic on eth0 | 2016-01-02 20:24:04 | 7.47 Kbps | -120.94 Kbps | Graph |

2 selected



- **Monitoring** → **Events**
 - When has a trigger thrown an alarm?
 - History of discovery actions.

ZABBIX Monitoring Inventory Reports Configuration Administration

Dashboard Overview Web Latest data Triggers Events Graphs Screens Maps Discovery IT services

Events Group: Zabbix servers Host: Zabbix server 1 Source: Trigger [Export to CSV](#)

Filter ▲

Trigger: Zabbix server 1: Zabbix agent on Zabbix server 1 is unreachable for 5 minutes [Select](#)

Filter Reset

Zoom: 5m 15m 30m 1h 2h 3h 6h 12h 1d 3d 7d All 2016-01-02 23:06 - 2016-01-11 23:08

«« 7d 1d 12h 1h 5m | 5m 1h 12h 1d 7d »» 9d 2m fixed

| TIME | HOST | DESCRIPTION | STATUS | SEVERITY | DURATION | ACK | ACTIONS |
|-------------------------------------|---------------------------------|--|---------|----------|-----------|-----|-------------------|
| 2016-01-03 20:31:43 | Zabbix server 1 | Zabbix agent on Zabbix server 1 is unreachable for 5 minutes | OK | Average | 8d 2h 36m | No | 1 |
| 2016-01-03 19:27:30 | Zabbix server 1 | Zabbix agent on Zabbix server 1 is unreachable for 5 minutes | PROBLEM | Average | 1h 4m 13s | No | 1 |
| 2016-01-02 23:22:21 | Zabbix server 1 | Zabbix agent on Zabbix server 1 is unreachable for 5 minutes | OK | Average | 20h 5m 9s | No | 2 |
| 2016-01-02 23:20:31 | Zabbix server 1 | Zabbix agent on Zabbix server 1 is unreachable for 5 minutes | PROBLEM | Average | 1m 50s | No | 2 |
| 2016-01-02 23:06:05 | Zabbix server 1 | Zabbix agent on Zabbix server 1 is unreachable for 5 minutes | OK | Average | 14m 26s | No | |

Displaying 5 of 5 found



Monitoring → Graphs, Screens

ZABBIX Monitoring Inventory Reports Configuration Administration

Dashboard Overview Web Latest data Triggers Events Graphs **Screens** Maps Discovery IT services

Screens Filters Edit screen

All screens / Zabbix server

Filter

Zabbix server 1: CPU load (1h)

| | [avg] | last | min |
|--|-------|------|-----|
| Processor load (1 min average per core) | 0.38 | 0.38 | 0.0 |
| Processor load (5 min average per core) | 0.15 | 0.15 | 0.0 |
| Processor load (15 min average per core) | 0.1 | 0.1 | 0.0 |

Data from history. Generated in 0.59 sec.

New host: CPU load (1h)

| | [avg] | last | min |
|--|-------|-------|-----|
| Processor load (1 min average per core) | 0.295 | 0.295 | 0.0 |
| Processor load (5 min average per core) | 0.58 | 0.58 | 0.0 |
| Processor load (15 min average per core) | 0.59 | 0.59 | 0.0 |

Data from history. Generated in 0.22 sec.

Zabbix server 1: CPU utilization (1h)

| | [avg] | last | min | avg |
|--------------------|--------|---------|------------|------------|
| CPU idle time | 94.9 % | 81.16 % | 93.27 % | 93.27 % |
| CPU user time | 1.84 % | 0.95 % | 2.26 % | 2.26 % |
| CPU system time | 1.58 % | 1.29 % | 2.03 % | 2.03 % |
| CPU iowait time | 1.39 % | 1.05 % | 2.13 % | 2.13 % |
| CPU nice time | 0 % | 0 % | 0 % | 0 % |
| CPU interrupt time | 0 % | 0 % | 0.000288 % | 0.000288 % |
| CPU softirq time | 0.41 % | 0.17 % | 0.33 % | 0.33 % |
| CPU steal time | 0 % | 0 % | 0 % | 0 % |

Data from history. Generated in 0.64 sec.

New host: CPU utilization (1h)

| | [avg] | last | min | avg |
|--------------------|----------|---------|-----------|-----------|
| CPU idle time | 68.12 % | 29.95 % | 56.49 % | 56.49 % |
| CPU user time | 25.92 % | 17.5 % | 35.42 % | 35.42 % |
| CPU system time | 7.11 % | 4.5 % | 6.87 % | 6.87 % |
| CPU iowait time | 1.03 % | 0.62 % | 1.16 % | 1.16 % |
| CPU nice time | 0.0085 % | 0 % | 0.01 % | 0.01 % |
| CPU interrupt time | 0 % | 0 % | 0.00383 % | 0.00383 % |
| CPU softirq time | 0.06 % | 0.03 % | 0.1 % | 0.1 % |
| CPU steal time | 0 % | 0 % | 0 % | 0 % |

Data from history. Generated in 0.72 sec.



- Monitoring → **Maps**

Maps Minimum severity [Edit map](#) [+](#) [↗](#)

All maps / Network

The map displays a network topology with the following components and status:

- Zabbix server**: OK
- Proxy 1**: Connected to Remote hosts and Firewall.
- Remote hosts**: OK
- Firewall**: Connected to Proxy 1 and Zabbix server.
- Host 1**: DISABLED
- Host 2**: MAINTENANCE (One time)
- New host 1 Problem**: 100MBps (Problem)

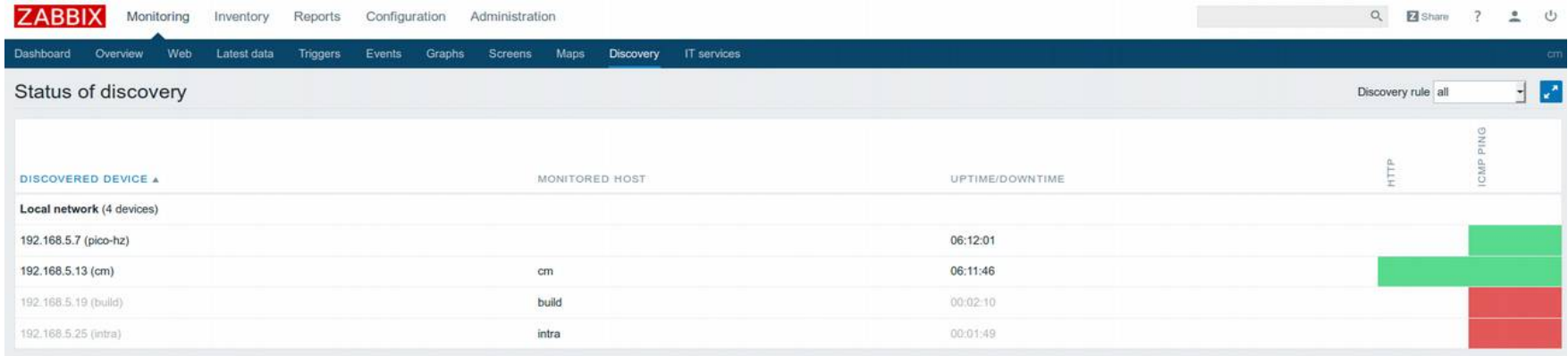
Context menu for 'New host 1 Problem':

- SCRIPTS
 - Detect operating system
 - Ping
 - Traceroute
- GO TO
 - Host inventory
 - Latest data
 - Triggers
 - Graphs
 - Host screens



- **Monitoring** → **Discovery**

- Results from automatic service discovery are shown on this screen, e.g. http, ftp, ssh, telnet, imap, NNTP, SNMP agents, Zabbix agents:





- Monitoring → IT Services
 - SLA information

ZABBIX Monitoring Inventory Reports Configuration Administration

Dashboard Overview Web Latest data Triggers Events Graphs Screens Maps Discovery IT services

IT services

Period: Last 7 days

| SERVICE | STATUS | REASON | PROBLEM TIME | SLA / ACCEPTABLE SLA |
|---|--------|--------|---|---------------------------|
| root | | | | |
| ▼ Servers | OK | | | |
| Server 1 - Zabbix agent on Zabbix server 1 is unreachable for 5 minutes | OK | | <div style="width: 100%; height: 10px; background-color: green;"></div> | 0.1248 99.8752 / 99.9000 |
| Server 2 | OK | | <div style="width: 100%; height: 10px; background-color: green;"></div> | 0.0000 100.0000 / 99.9000 |
| Server 3 | OK | | <div style="width: 100%; height: 10px; background-color: green;"></div> | 0.0000 100.0000 / 99.9000 |
| Server 4 | OK | | <div style="width: 100%; height: 10px; background-color: green;"></div> | 0.0000 100.0000 / 99.9000 |
| Server 5 | OK | | <div style="width: 100%; height: 10px; background-color: green;"></div> | 0.0000 100.0000 / 99.9000 |
| ▶ Business system | OK | | | |
| ▶ Network service | OK | | | |
| ▶ Public cloud service | OK | | | |



- **Inventory** → **Overview, Hosts**
 - CFDB-like
- **Reports** →
 - **Status of Zabbix**
 - **Availability Report**
 - Shows availability of every item over time.
 - **Triggers top 100**
 - Find the triggers with the most often status changes.
 - **Audit**
 - See the changes done per user within the Zabbix system.
 - **Action log**

Action log

Filter ▲

Recipient Select

Zoom: 5m 15m 30m 1h 2h 3h 6h 12h 1d 3d 7d 14d 1m All Filter Reset 2015-08-21 16:44 - 2015-11-03 11:24 (now)

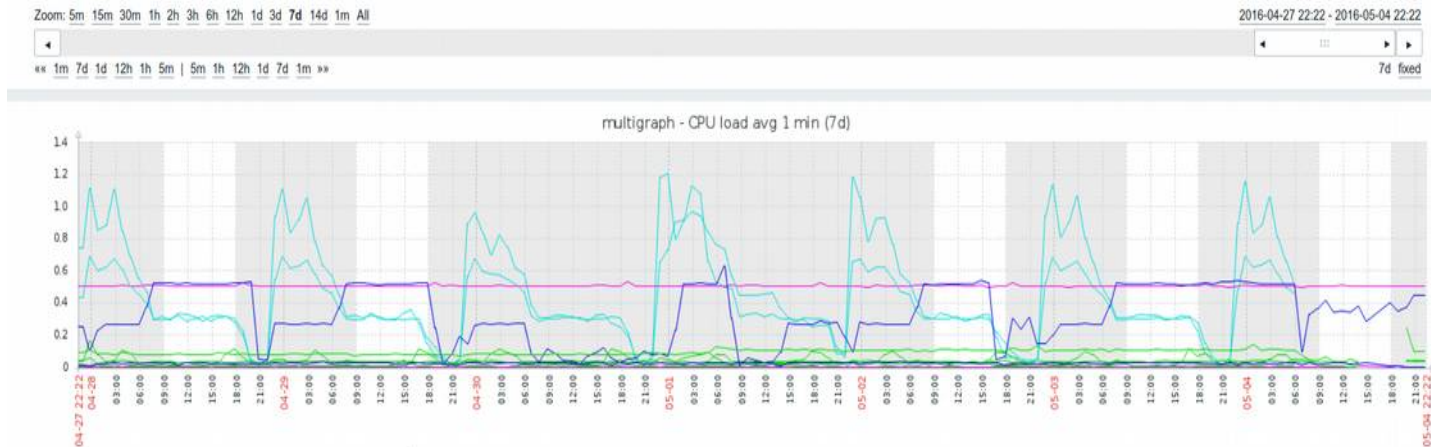
◀ ▶

== 1m 7d 1d 12h 1h 5m | 5m 1h 12h 1d 7d 1m == 2m 13d 18h 40m fixed

| TIME | ACTION | TYPE | RECIPIENT(S) | MESSAGE | STATUS | INFO |
|---------------------|--|-------|--|--|--------|------|
| 2015-08-26 12:16:49 | Report problems to Zabbix administrators | Email | Admin (Zabbix Administrator) Martins.Valkovskis@zabbix.com | Subject: OK: Disk I/O is overloaded on New host Message: Trigger: Disk I/O is overloaded on New host Trigger status: OK Trigger severity: Warning Trigger URL: Item values: 1. CPU iowait time (New host:system.cpu.utl[iowait]): 1.61 % 2. "UNKNOWN" ("UNKNOWN":"UNKNOWN"): "UNKNOWN" 3. "UNKNOWN" ("UNKNOWN":"UNKNOWN"): "UNKNOWN" Original event ID: 19870 | Sent | |
| 2015-08-26 12:16:49 | Report problems to Zabbix administrators | Email | Admin (Zabbix Administrator) Martins.Valkovskis@zabbix.com | Subject: PROBLEM: Disk I/O is overloaded on New host Message: Trigger: Disk I/O is overloaded on New host Trigger status: PROBLEM Trigger severity: Warning Trigger URL: Item values: 1. CPU iowait time (New host:system.cpu.utl[iowait]): 32.64 % | Sent | |



- **Configuration** → **Host groups**
 - Group hosts into host groups. One host can be assigned to multiple host groups.
- **Configuration** → **Templates**
 - Templates are pre-configured configurations, which can be assigned to host.
 - A Template consists of
 - Applications
 - Items (= metrics), e.g. **“CPU iowait”**
 - Triggers (= alarms), e.g. **“Disk I/O is overloaded on {HOST.NAME}”**
 - Graphs: pre-configured graph to show some selected metrics
 - Screens:
 - Pre-configured page to show multiple graphs on one page / system
 - Very useful are graphs or screens, which show a given metric for a host group:





- **Configuration** → **Templates**
 - **Discovery (LLD – Low Level Discovery)**

The screenshot shows the Zabbix web interface. At the top, there is a navigation menu with 'ZABBIX' in a red box, followed by 'Monitoring', 'Inventory', 'Reports', 'Configuration', and 'Administration'. Below this is a secondary menu with 'Host groups', 'Templates', 'Hosts', 'Maintenance', 'Actions', 'Discovery', and 'IT services'. The main content area is titled 'Discovery rules' and includes a 'Create discovery rule' button. Below the title is a breadcrumb trail: 'All templates / Template OS Linux / Applications 10 / Items 32 / Triggers 15 / Graphs 5 / Screens 1 / Discovery rules 2 / Web scenarios'. A table lists the discovery rules with columns for NAME, ITEMS, TRIGGERS, GRAPHS, HOSTS, KEY, INTERVAL, TYPE, and STATUS. Two rules are shown: 'Mounted filesystem discovery' and 'Network interface discovery', both with a status of 'Enabled'. At the bottom left, it says '0 selected' and provides 'Enable', 'Disable', and 'Delete' buttons.

| NAME | ITEMS | TRIGGERS | GRAPHS | HOSTS | KEY | INTERVAL | TYPE | STATUS |
|------------------------------|-------------------|----------------------|--------------------|-----------------|------------------|----------|--------------|---------|
| Mounted filesystem discovery | Item prototypes 5 | Trigger prototypes 2 | Graph prototypes 1 | Host prototypes | vfs.fs.discovery | 1h | Zabbix agent | Enabled |
| Network interface discovery | Item prototypes 2 | Trigger prototypes | Graph prototypes 1 | Host prototypes | net.if.discovery | 1h | Zabbix agent | Enabled |



- **Configuration** → **Hosts**
 - Interface configuration
 - Templates can be linked hierarchical or just plain
 - Monitoring can be done agentless, Zabbix agent based, SNMP, JMX, IPMI
 - Zabbix 3.0 supports TLS encrypted agent-server configurations.
 - How to create new hosts:
 - Manually
 - Clone an existing host
 - Import an XML-based host configuration
 - E.g. define a **discovery rule** to detect hosts either through ICMP, Zabbix agent or s.th. else. Define an **action** to assign all discovered hosts to host group xyz and link template T.

| NAME | APPLICATIONS | ITEMS | TRIGGERS | GRAPHS | DISCOVERY | WEB | INTERFACE | TEMPLATES | STATUS | AVAILABILITY | INFO | AGENT ENCRYPTION |
|--|-----------------|----------|-------------|-----------|-------------|-------|---------------------|---|---------|-------------------|------|------------------|
| <input type="checkbox"/> Zabbix server | Applications 12 | Items 71 | Triggers 44 | Graphs 12 | Discovery 2 | Web 1 | 192.168.3.194:10050 | Template1 (Template2), Template App Zabbix Server, Template OS Linux (Template App Zabbix Agent) | Enabled | ZBX SNMP JMX IPMI | | NONE |
| <input type="checkbox"/> procurve.zabbix.lan | Applications 1 | Items 1 | Triggers | Graphs | Discovery 1 | Web | 192.168.3.7:161 | Template SNMP Interfaces | Enabled | ZBX SNMP JMX IPMI | | NONE |
| <input type="checkbox"/> New host | Applications 10 | Items 42 | Triggers 18 | Graphs 9 | Discovery 2 | Web | 192.168.3.31:32050 | Template OS Linux (Template App Zabbix Agent) | Enabled | ZBX SNMP JMX IPMI | | NONE |



- **Configuration** → **Hosts**
 - 2nd optional host name
 - Assign host groups
 - Optional:
 - Select proxy, assign templates, configure IPMI, macros and encryption (agent → server, server → agent)

ZABBIX Monitoring Inventory Reports Configuration Administration

Host groups Templates Hosts Maintenance Actions Discovery IT services

Hosts

All hosts / cm Enabled ZBX SNMP JMX IPMI Applications 14 Items 61 Triggers 50 Graphs 27 Discovery rules 2 Web scenarios

Host Templates IPMI Macros Host inventory Encryption

Host name:

Visible name:

Groups

In groups: all, all-linux, all-ubuntu, Zabbix servers, zone-hz

Other groups: all-centos, all-kali, all-network

New group:

Agent interfaces

| IP ADDRESS | DNS NAME | CONNECT TO | PORT | DEFAULT |
|--|----------------------|------------|-------|----------------------------------|
| <input type="text" value="127.0.0.1"/> | <input type="text"/> | IP DNS | 10050 | <input checked="" type="radio"/> |

[Add](#)

SNMP interfaces

| | | | | |
|--|----------------------|--------|-----|----------------------------------|
| <input type="text" value="127.0.0.1"/> | <input type="text"/> | IP DNS | 161 | <input checked="" type="radio"/> |
|--|----------------------|--------|-----|----------------------------------|

Use bulk requests

[Add](#)

JMX interfaces

| | | | | |
|--|----------------------|--------|-------|----------------------------------|
| <input type="text" value="127.0.0.1"/> | <input type="text"/> | IP DNS | 12345 | <input checked="" type="radio"/> |
|--|----------------------|--------|-------|----------------------------------|

[Add](#)

IPMI interfaces

| | | | | |
|--|----------------------|--------|-----|----------------------------------|
| <input type="text" value="127.0.0.1"/> | <input type="text"/> | IP DNS | 623 | <input checked="" type="radio"/> |
|--|----------------------|--------|-----|----------------------------------|

[Add](#)

Description:

Monitored by proxy:

Enabled:

[Update](#) [Clone](#) [Full clone](#) [Delete](#) [Cancel](#)



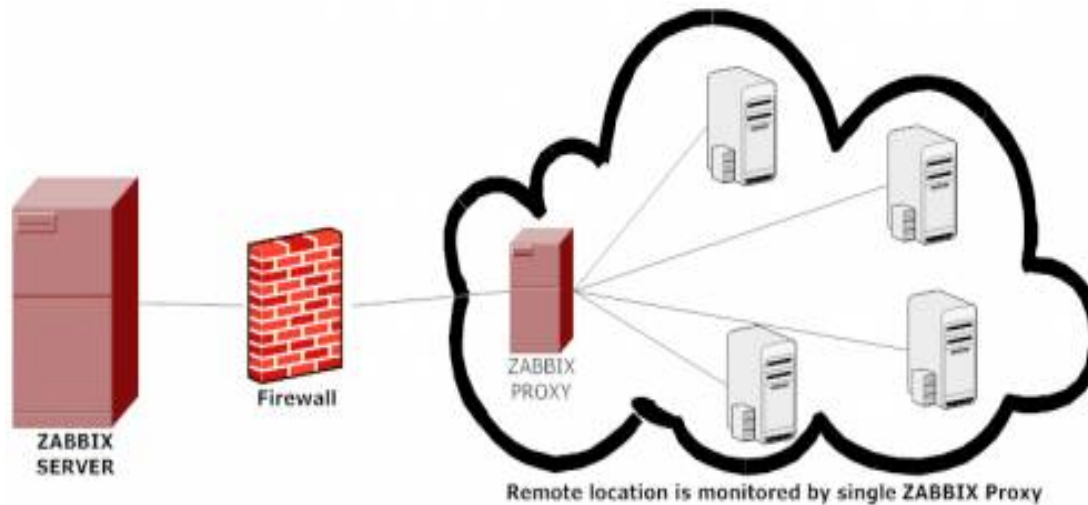
.... we skip over

- Configuration → **Maintenance**
- Configuration → **Actions**
- Configuration → **Discovery**
- Configuration → **IT services**

and talk about the Zabbix architecture, how to make Zabbix high available.
We get some ideas if and how Zabbix scales...

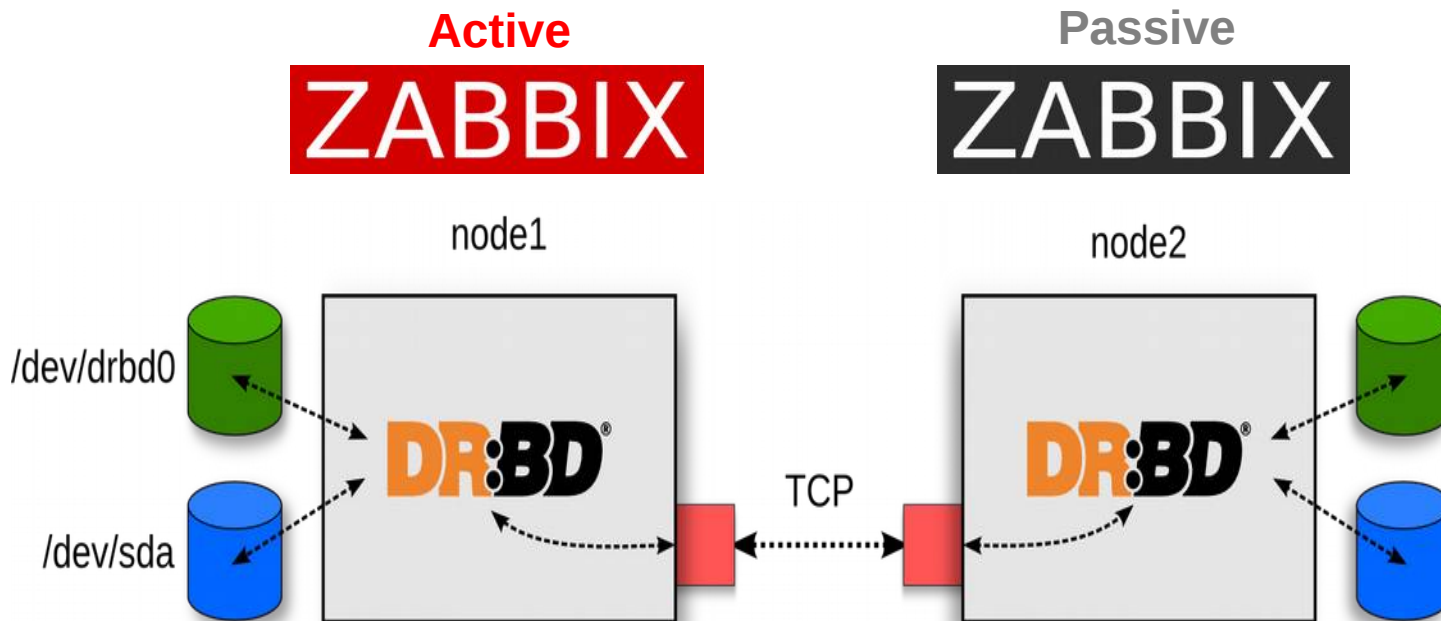


- Zabbix proxies
 - The traffic between the server and proxy is bundled into one TCP connection
 - The proxy can buffer monitoring data for some time
 - The Zabbix proxy does not process triggers, events or alerts.
 - The proxy can use an sqlite database, which make the proxy very lightweight





- Zabbix agent
 - https://www.zabbix.com/documentation/3.0/manual/config/items/itemtypes/zabbix_agent
 - Agent.* , kernel.* log[], net.* , proc.* , sensor[], system.* , vfs.* , vm.* , web.*
 - Functionality can be extended through scripts
 - A script can be assigned to a Zabbix key
 - This key-script mapping is configured under the Zabbix agent in
 - The key can be immediately used on the Zabbix server to trigger the execution of the mapped script





- TLS encryption (formerly external: SSH forwarding, stunnel or VPN)
- New GUI since 3.0
- The GUI will even be better in upcoming releases, e.g. a user will be able to create its own pages or extend existing ones
- Individual maps, screens, slideshows
- Different conditions/thresholds for problem state and recovery states / trigger hysteresis
- Automatic anomaly detection based on time slots
- Problem/trend prediction



Beats, JDBC/JMX, Shell-Scripts, Windows Event Log, Application Logs, Graylog/_log4j, http/http POST, http_poller, syslog/RELP, REDIS (Logstash), SNMP, tcp, udp, websockets



