Zabbix 3.0

The Simple, the Powerful and the Shiny
by
Zabbix SIA – www.zabbix.com

IntelliTrend IT-Services GmbH

Otto-Brenner-Strasse 119

D-33607 Bielefeld

Germany

Contact: Wolfgang Alper

Email: wolfgang.alper@intellitrend.de

www.intellitrend.de

Zabbix - “The Simple”

- Mature All-In-One monitoring solution
- Packaged for every major Linux distribution
- Easy to setup
- Out-of-the-box templates for Linux, Windows and SNMP devices

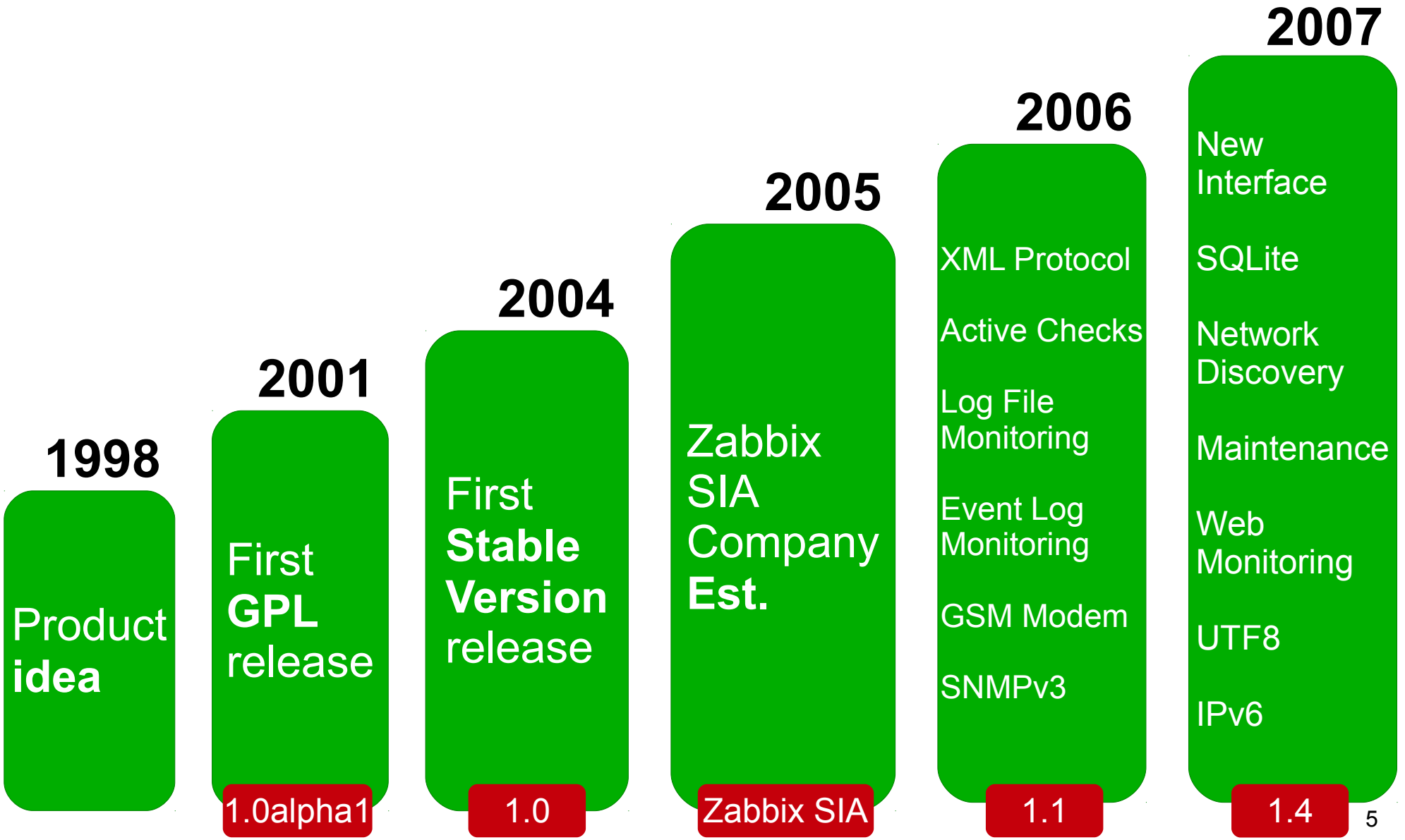
Zabbix - “The Powerful”

- Monitoring of millions of items
- Monitoring of thousands of hosts
- Distributed Monitoring across networks
- Template system to unify configurations
- Flexible escalation management
- API to integrate 3th party applications and command line tools

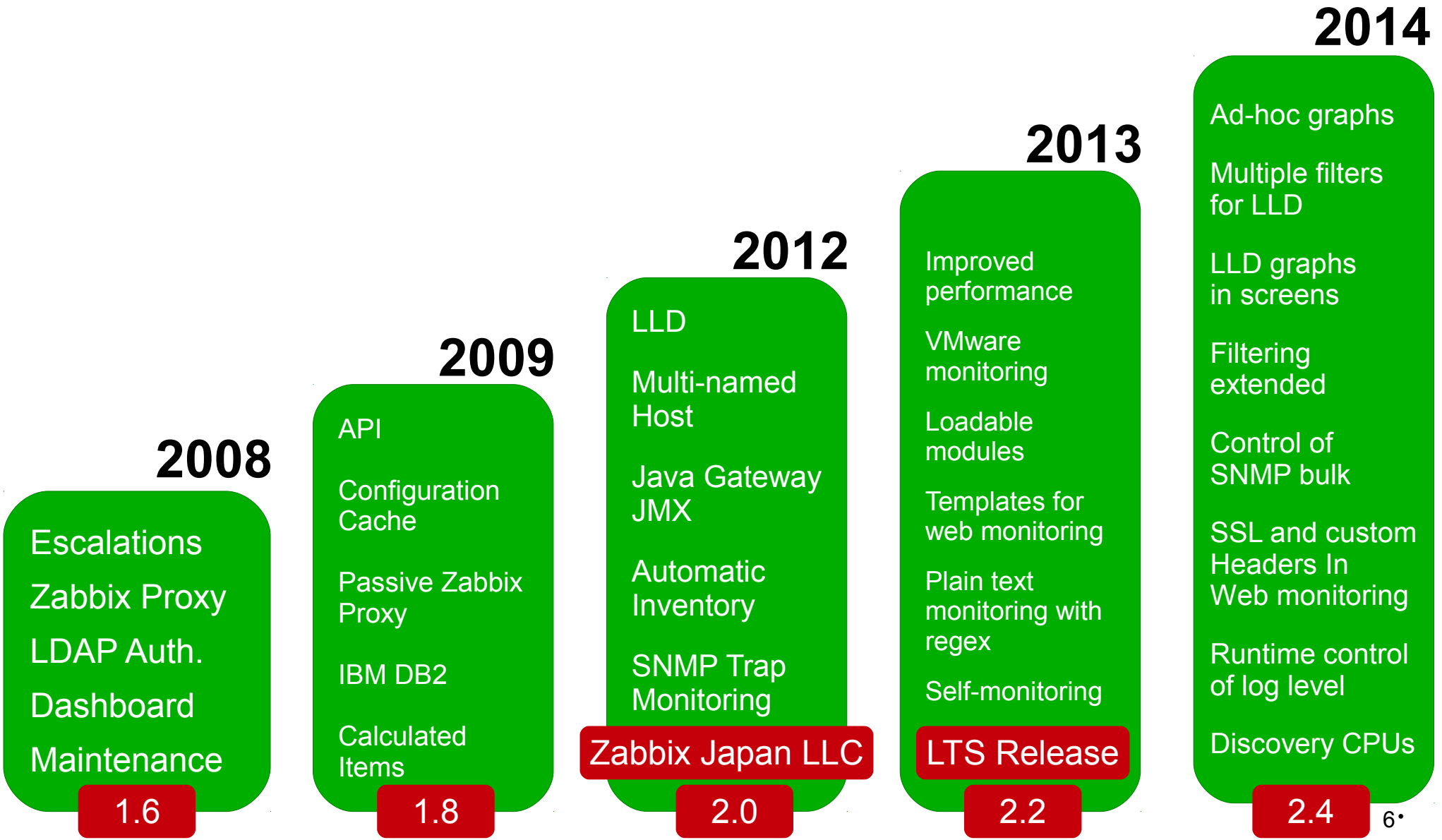
Zabbix - “The Shiny”

- Continuous development over 15+ years
- True open source, no “Enterprise” or “Professional” version
- LTS (Long Term Support) versions
- Regular product updates and bugfixes
- Enterprise-friendly support pricing
- Commercially backed

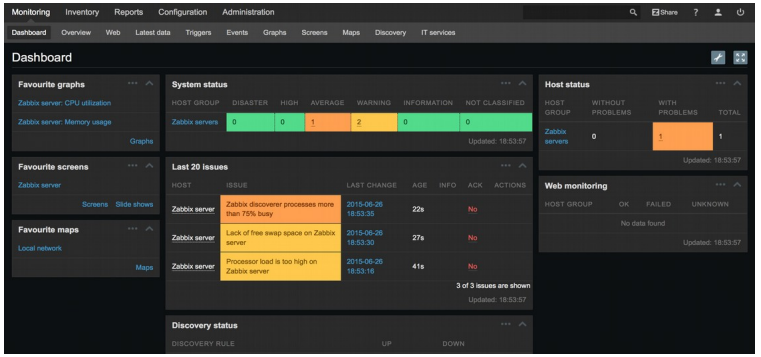
Zabbix - History



Zabbix - History



How Zabbix works



Visualization

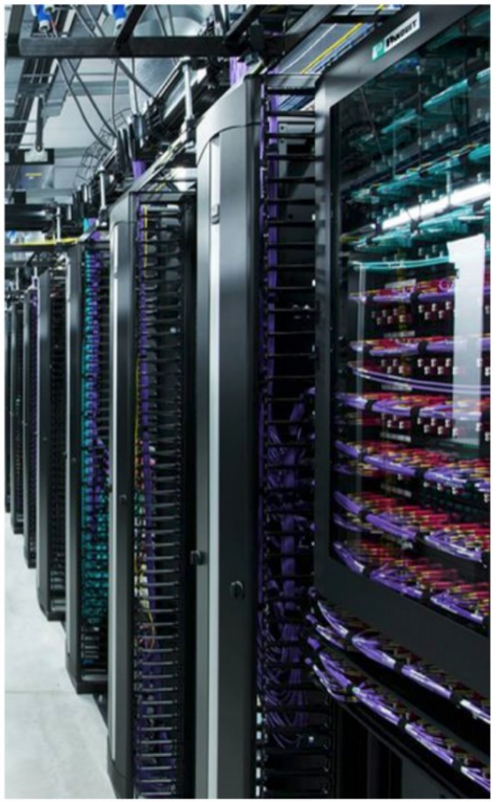
Notifications

DATABASE

History

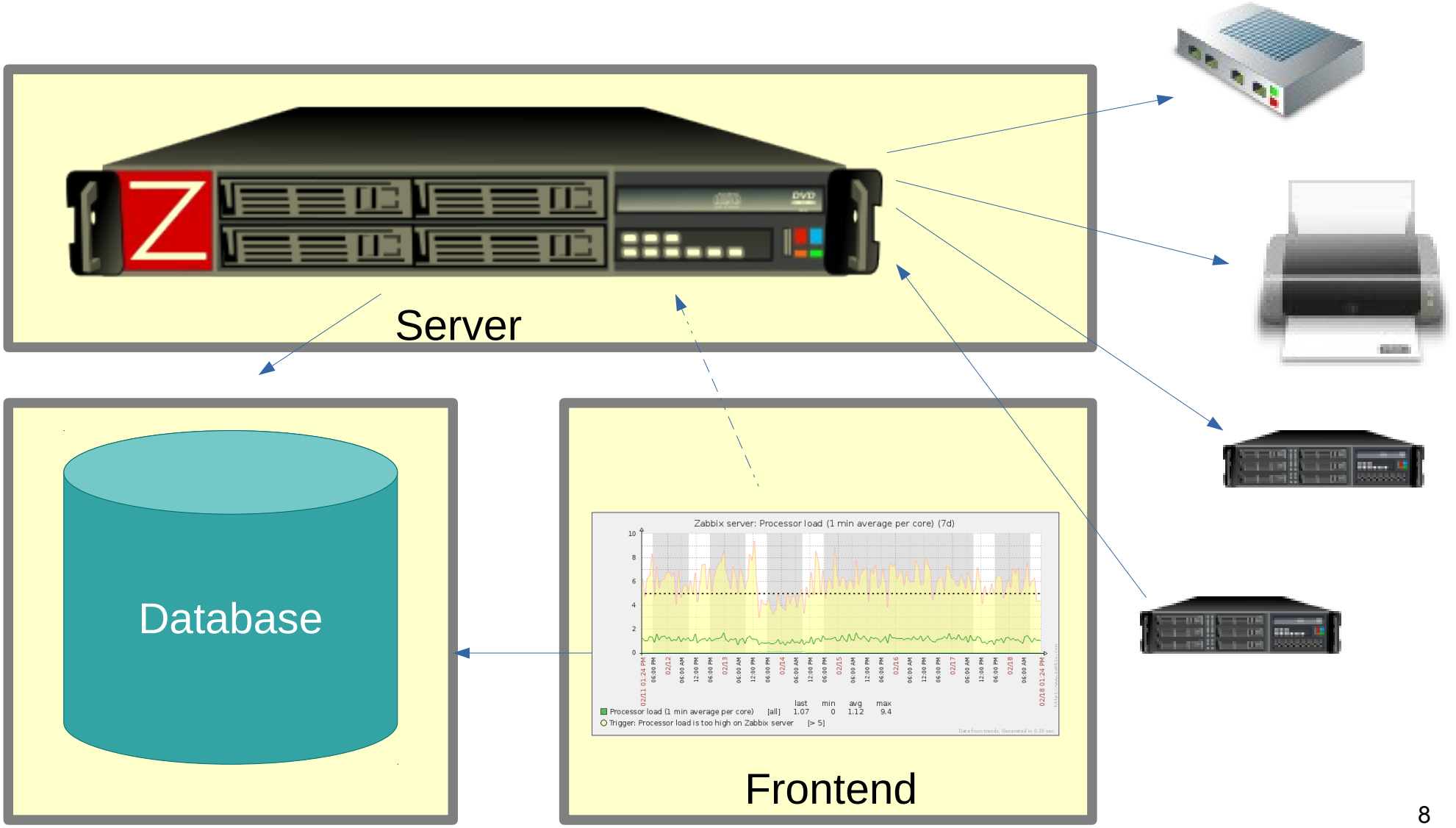
ZABBIX SERVER

Analysis

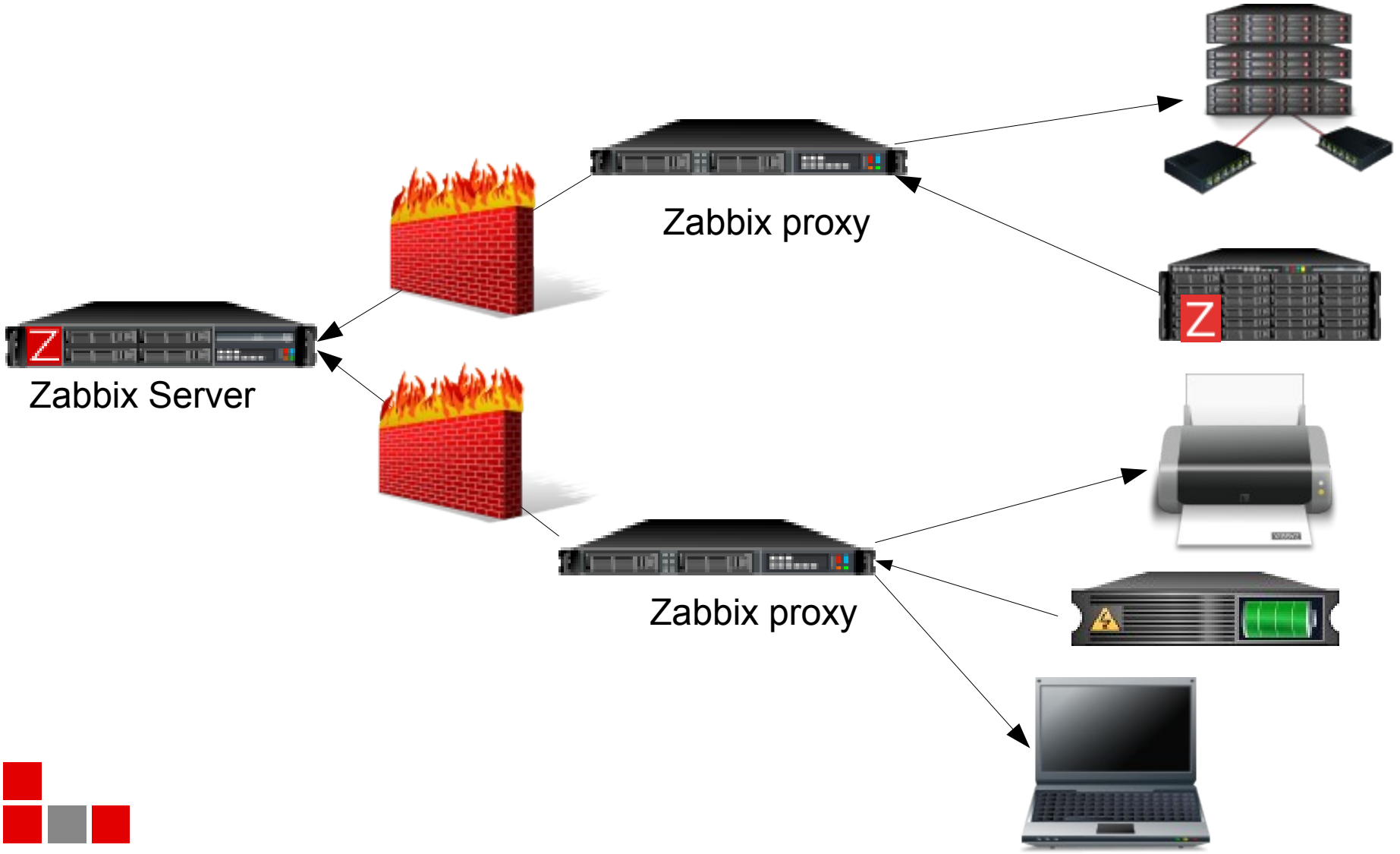


Data

Zabbix – Architecture



Distributed Monitoring



Item types - agent(based/less)

Zabbix agent
- Server polls

Zabbix agent (active)
- Processed by Zabbix agent
- Can be cached

Agent-less checks (simple)
- Performed by Zabbix server

SNMP agent/trapper
- All SNMP versions supported

Zabbix trapper
- Used with Zabbix sender

Internal
- Zabbix health

Vmware Collector (single poll)
- Hypervisor + Vm's

Web Monitoring

IPMI

JMX

Aggregate

grpsum["MySQL Servers", "vfs.fs.size[/,total]","last","0"]

External check

script[parameters]

SSH
- Password and key authentication supported

Telnet

Database

Calculated

last("vm.memory.size[free]") +last("vm.memory.size[buffers]")

Agent capabilities

Common items

- CPU
- Memory
- Filesystem
- Logfiles
- ...more than 70+ things built-in

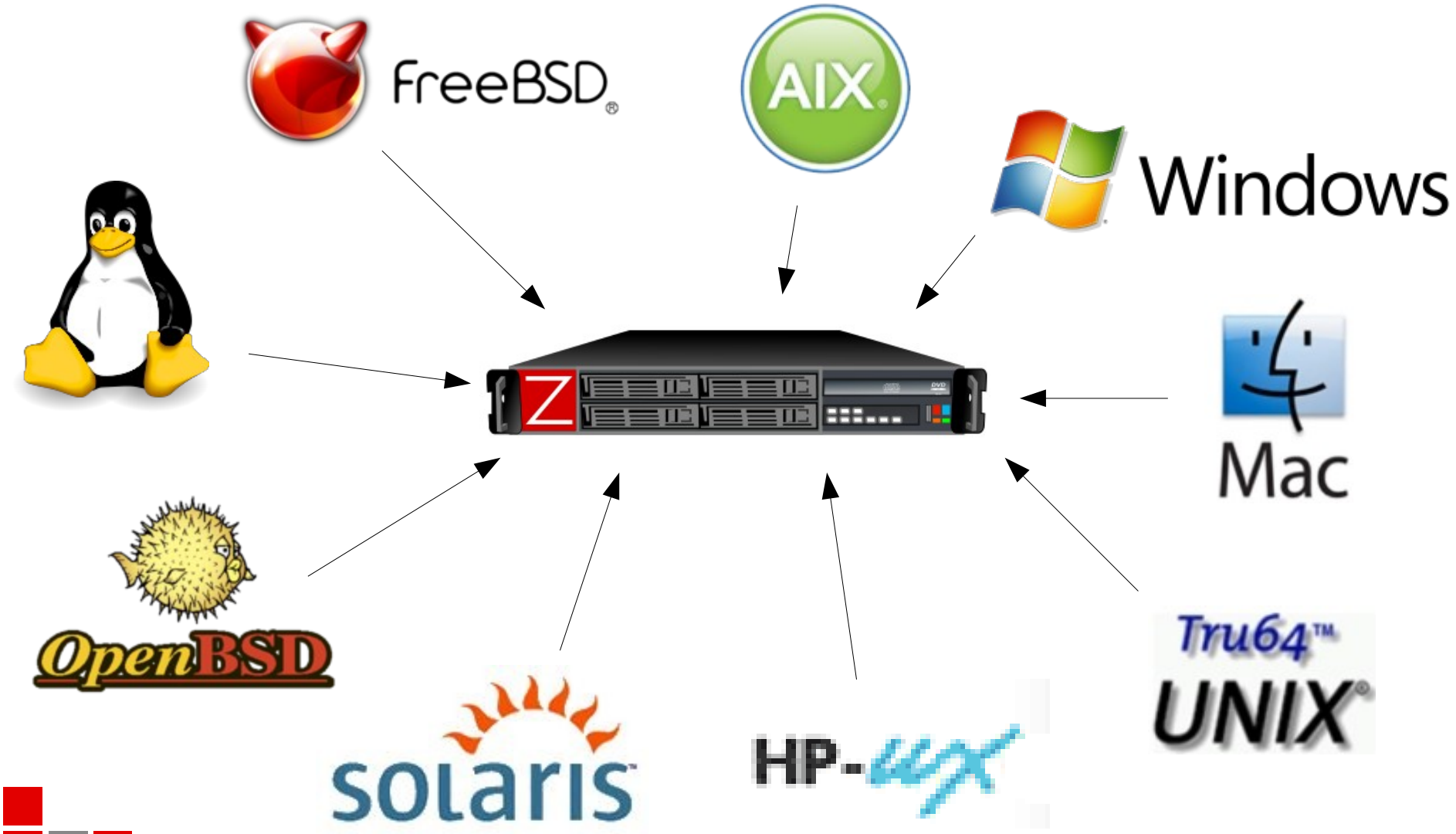
```
proc.num[inetd]
proc.mem[inetd]
system.cpu.switches
system.cpu.intr
system.cpu.util[all,user,avg1]
system.cpu.load[all,avg1]
system.cpu.num[online]
system.cpu.discovery
system.uname
system.hw.chassis
system.hw.cpu
```

OS specific items

- Windows – Perfmon Interface
- Windows – WMI Interface
- Linux/FreeBSD – kernel.maxproc
- Linux/FreeBSD – vfs.fs.inode
- ...

```
[u|0]
[u|0]
[u|522013252]
[u|244599437]
[m|ZBX_NOTSUPPORTED] [Collector is not started.]
[d|0.080000]
[u|1]
[m|ZBX_NOTSUPPORTED] [Collector is not started.]
[s|Linux rich 3.14.3 #2 Wed May 7 12:20:42 CDT 2014
[s|
[t|processor 0: GenuineIntel Intel(R) Pentium(R) D C
```

Agent availability



Trigger definitions

What's a problem?

Extremely flexible problem conditions

- Check multiple values
- Comparison, math, boolean logic

Functions last, min, max, avg, delta, time etc.

6 Severity levels

Trigger definitions

Detecting problems – really flexible:

- Average over last 10 minutes
- Count of matching values over last 30 minutes
- Average for the last hour relative to the same hour day/two days/week ago
- Check multiple hosts (i.e. Mailserver for mx 10, mx 20)

Trigger definitions

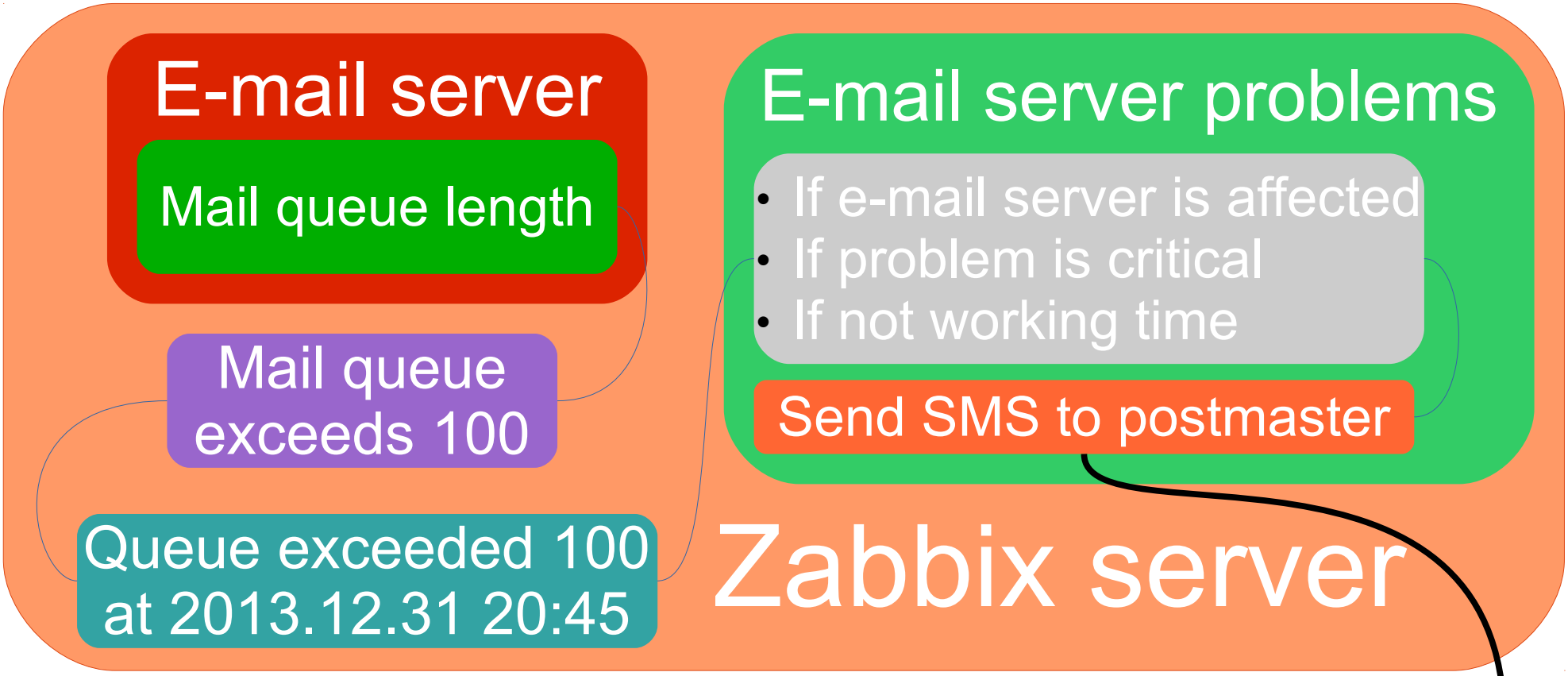
Examples:

- Over time:
  {lin-srv1:system.cpu.load.min(10m)}>5

- Over number of checks:
  {lin-srv1:system.cpu.load.min(#10)}>5

- Over multiple hosts:
  {lin-srv1:system.cpu.load.min(10m)}>5
  &
  {lin-srv2:system.cpu.load.min(10m)}>5

Workflow - Item to Operation



Host | Trigger | Condition | Operation

Item | Event | Action | Actual course taken

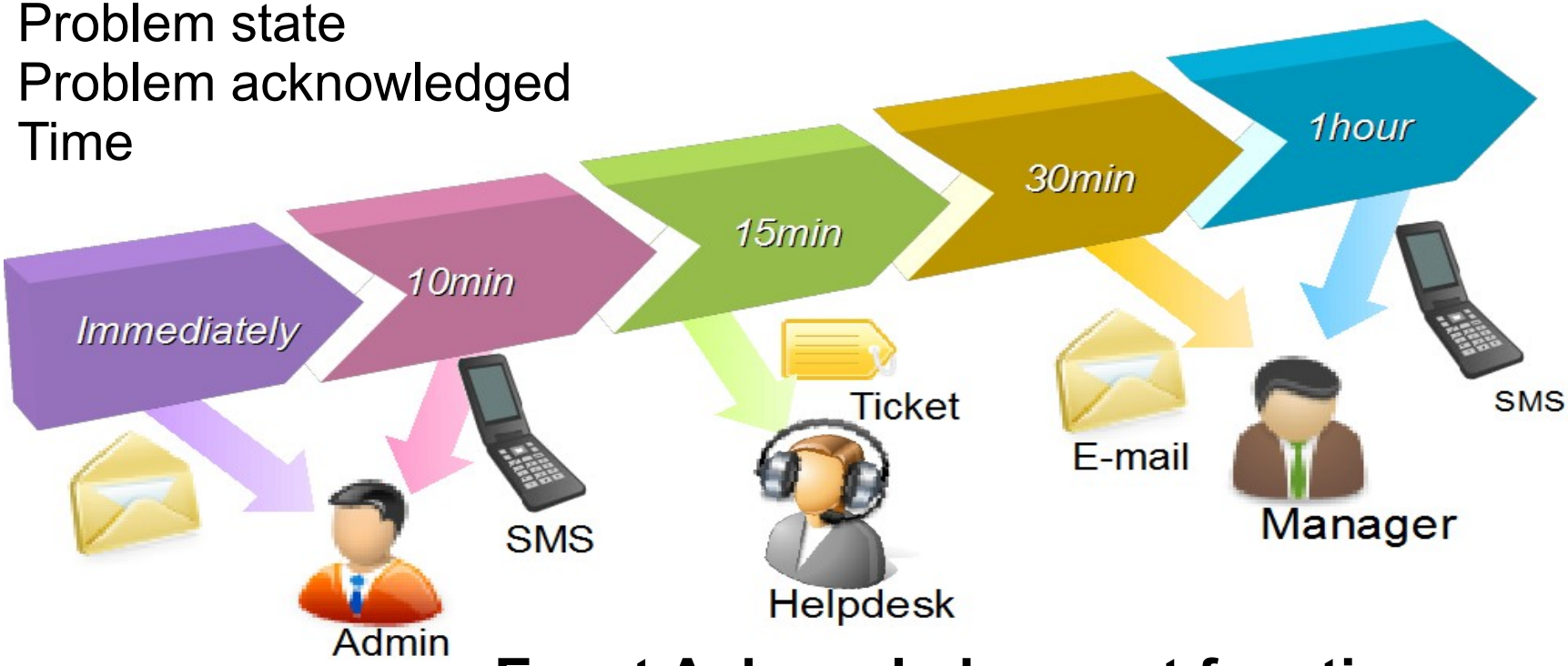
Notifications - Escalations

Escalation rules based on:

- Severity
- Hostname / Hostgroup
- Triggername / State
- Problem state
- Problem acknowledged
- Time

Notification methods:

- E-mail and/or SMS
- Chat message via Jabber
- Command execution



Event Acknowledgement function available to sync also with external tools

Templating

Templates:

- Manage configuration across multiple hosts
- Allow (userdefined) macro usage on global, template and host level {HOST.NAME}, {INVENTORY.LOCATION}, {$MAX_CPU_LOAD}
- Can be used in Autodiscovery rules
- Can be imported/exported via xml files

Templates include:

- Items
- Triggers
- Graphs
- Macros
- Screens

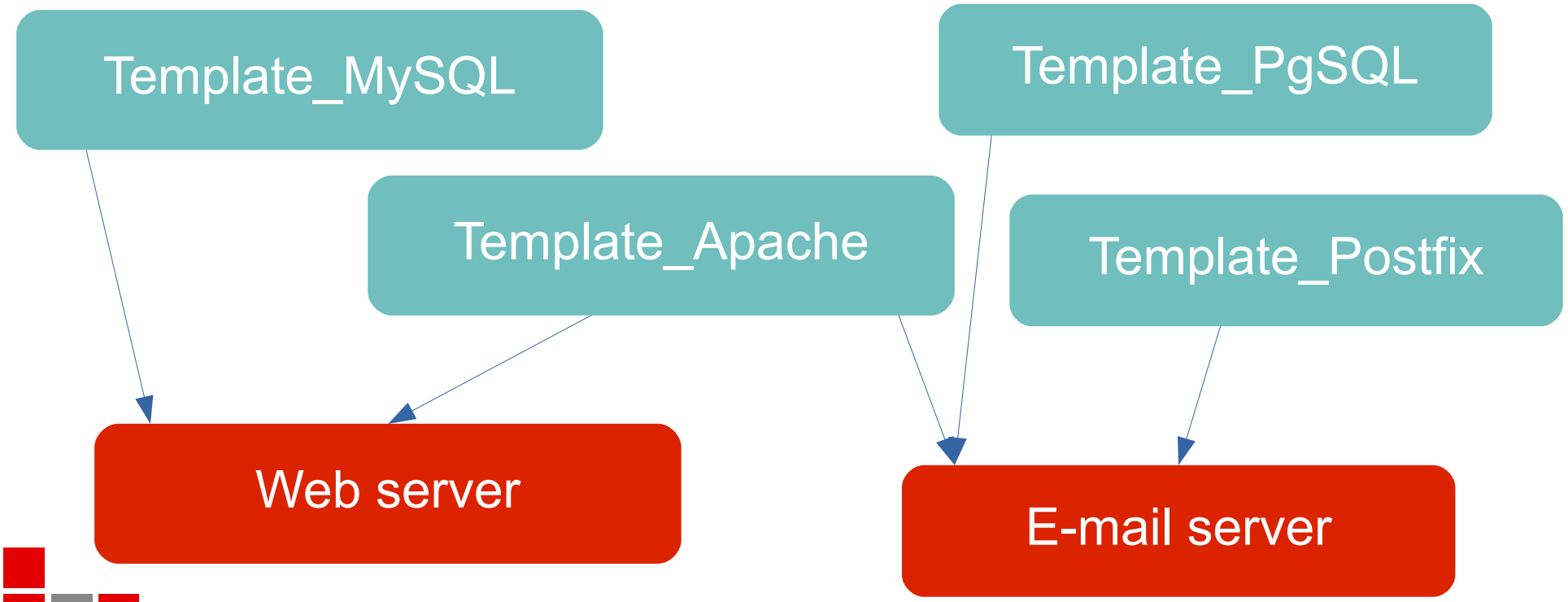
Template_MySQL

Template_Apache

Template_Postfix

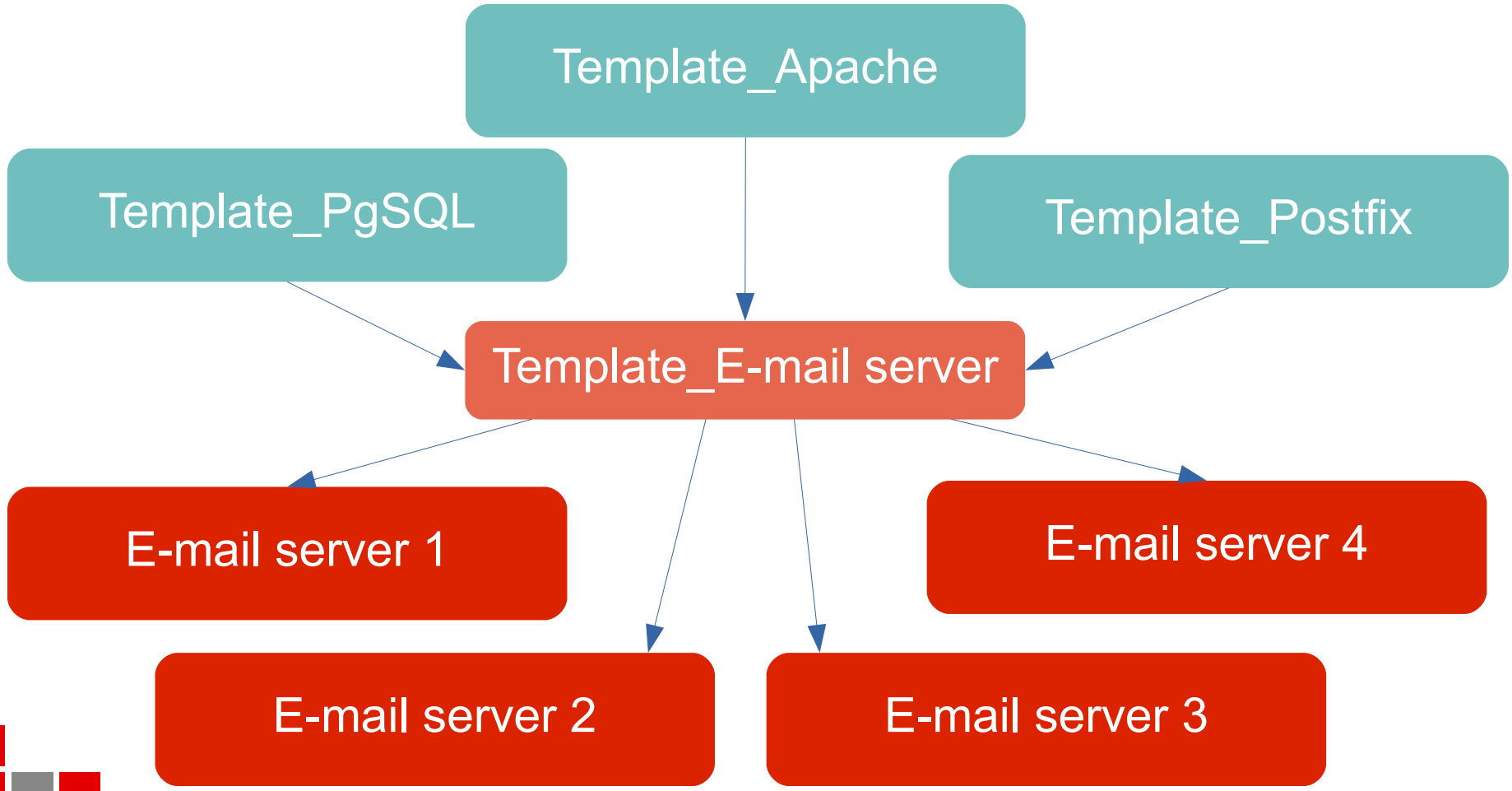
Templating

Templates allow combinations:



Templating

… and Templates allow nesting:



Extendability

- Run any command as an item to return a value
- Run any command on the agent
- Run any command on the server
- Run any command in response to events
- Feed (timestamped) data in Zabbix from custom scripts or 3th party apps
- No language restrictions

Extendability - Feed data

- Send single value

```
> zabbix_sender -z 10.11.12.13 -s "Shop 13" -k customer.count -o 113
```

- Send multiple values with timestamps at once from a file

```
"Shop 13" customer.count 1393393587 123
"Shop 12" customer.count 1393393587 19
"Shop 11" customer.count 1393393587 45
"Shop 10" customer.count 1393393587 87
"Shop 09" customer.count 1393393587 13
"Shop 08" customer.count 1393393587 66
```

Automation

- Auto Discovery
- Auto Registration
- Low Level Discovery
- XML import / export
- API

Automation via API
...beyond autodiscover

JSON-RPC API gives access to nearly any functionality

```
POST http://company.com/zabbix/api_jsonrpc.php HTTP/1.1
Content-Type: application/json-rpc

{"jsonrpc":"2.0","method":"apiinfo.version","id":1,"auth":null,"params":{}}
```

Example “host.get”

```
{
    "jsonrpc": "2.0",
    "method": "host.get",
    "params": {
        "output": [
            "hostid",
            "host"
        ],
        "selectInterfaces": [
            "interfaceid",
            "ip"
        ]
    },
    "id": 2,
    "auth": "0424bd59b807674191e7d77572075f33"
}
```

Request

=>

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "hostid": "10084",
            "host": "Zabbix server",
            "interfaces": [
                {
                    "interfaceid": "1",
                    "ip": "127.0.0.1"
                }
            ]
        }
    ],
    "id": 2
}
```

Response

Zabbix - Next LTS Version

3.0

Cleanup

Zabbix 3.0 Cleanup

TCP support for DNS items

```
net.dns.record[10.11.12.13,zabbix.com,,,,tcp]
```

Zabbix 3.0 Cleanup

API enhancements

```
{
    "usrgrpid": "7",
    "name": "Zabbix administrators",
    "rights": [
        {
            "permission": "3",
            "id": "2"
        }
    ]
}
```

Zabbix 3.0 Cleanup

LLD enhancements for trigger dependencies

Zabbix 3.0 Cleanup

XML versioning

```
<?xml version="1.0" encoding="UTF-8"?>
<zabbix_export>
  <version>2.0</version>
  <date>2013-11-12T16:13:38Z</date>
  <groups>
    <group>
      <name>Templates</name>
    </group>
  </groups>
  <templates>
    <template>
      <template>Template App Zabbix Proxy</template>
```

Zabbix 3.0 Cleanup

IPV6 for Java gateway

2001:0db8:0000:0042:0000:8a2e:0370:7334

+

Zabbix 3.0 Cleanup

General frontend cleanup

- Rewritten codebase to even use more MVC
- Extendable frontend code
- More POST instead of GET

Zabbix 3.0 Cleanup

Inventorise the inventory

- Default host inventory mode
- Changing it via discovery actions

For network discovery and active agents

Maintenance

Zabbix 3.0 Maintenance

Execute at runtime

```
$ zabbix_server
        --runtime-control
                housekeeper_execute
```

Collect, process

Zabbix 3.0
Collect, process

More memory monitoring

proc.mem[,,,,**<memtype>**]
- VmSize
- VmRSS
- VmData

Zabbix 3.0
Collect, process

Improved logfile monitoring

- Better performance
- More reliable
- Extract information and process as numeric value if needed.
- Effects Linux/Unix Logs + Windows Eventlogs

Zabbix 3.0
Collect, process

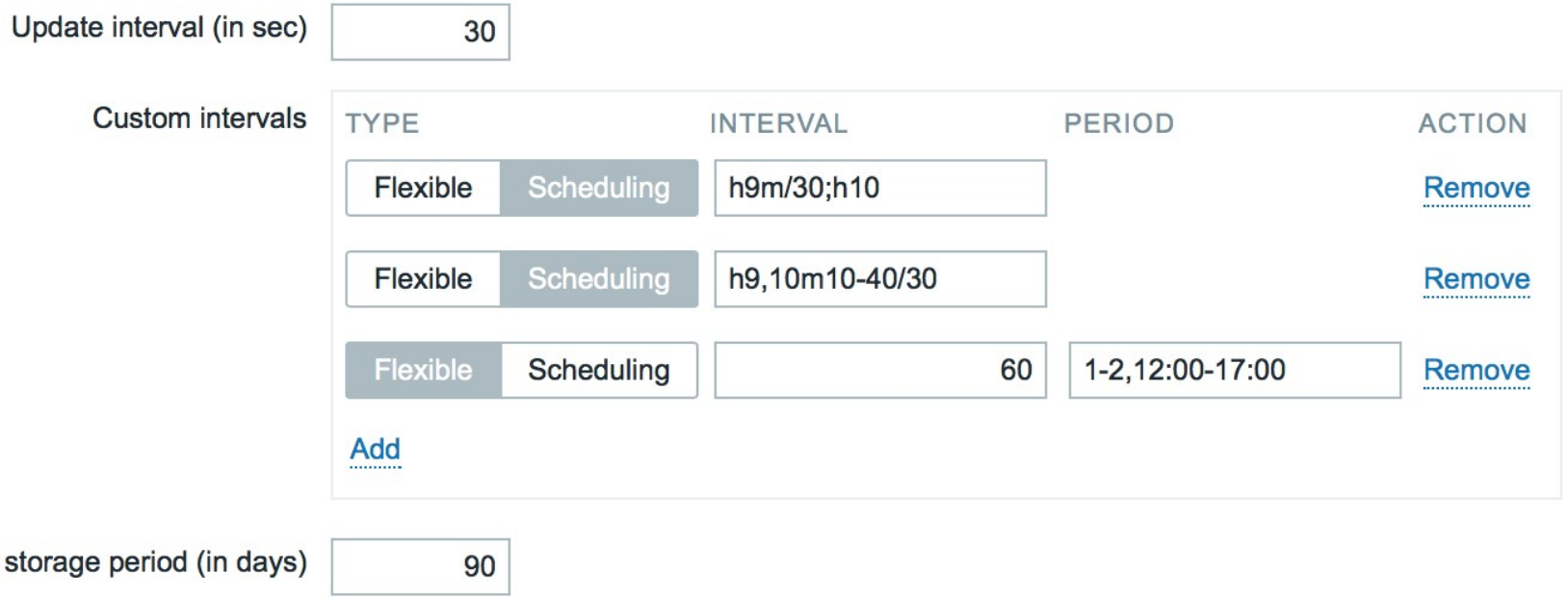
Per-process CPU usage

```
proc.cpu.util
[<name>,<user>,<type>,<cmdline>,<mode>,<zone>]
```

Zabbix 3.0
Collect, process

Crontab like item scheduling

m/5 - every five minutes
h9-17/2 - every 2 hours starting with 9:00 until 17:00
m0,30 or m/30 - hourly at hh:00 and hh:30



Zabbix 3.0
Collect, process

Percentile

percentile(1h,,95)
- In graphs
- In triggers
- In calculated items

About Percentile:
Percentile is a function used to determine the percent of acceptability.

The 95th percentile is the value which is greater than 95% of the observed values.

Example: 10 data values {3, 6, 7, 8, 8, 10, 13, 15, 16, 20}

25th = 3th number = 7
50th = 5th number = 8
75th = 8th number = 15
100th = last number = 20

Prediction

Zabbix 3.0 Prediction

A view to the future...

forecast()

- In the specified time, what will be the value?

Example:
{Zabbix server:vfs.fs.size[/,free].forecast(7d,,7d)}<100M

Zabbix 3.0 Prediction

Is there time left?

timeleft()

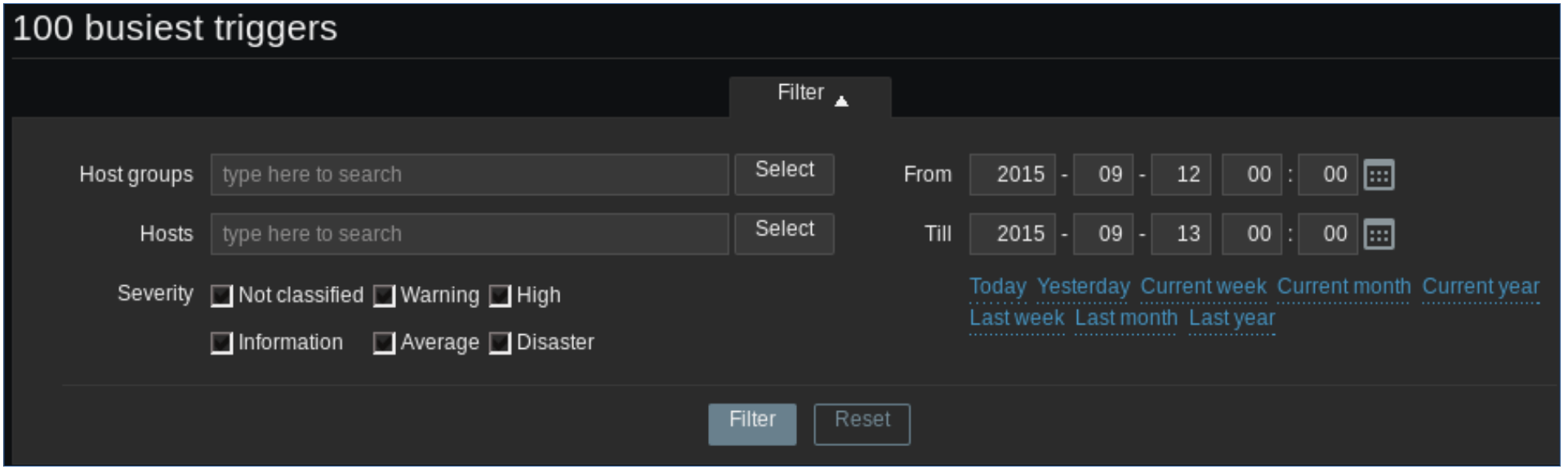
- How much time left until the specified threshold will be reached?

{Zabbix server:vfs.fs.size[/,free].timeleft(7d,,104857600)}<1h

Frontend usability

Zabbix 3.0
Frontend usability

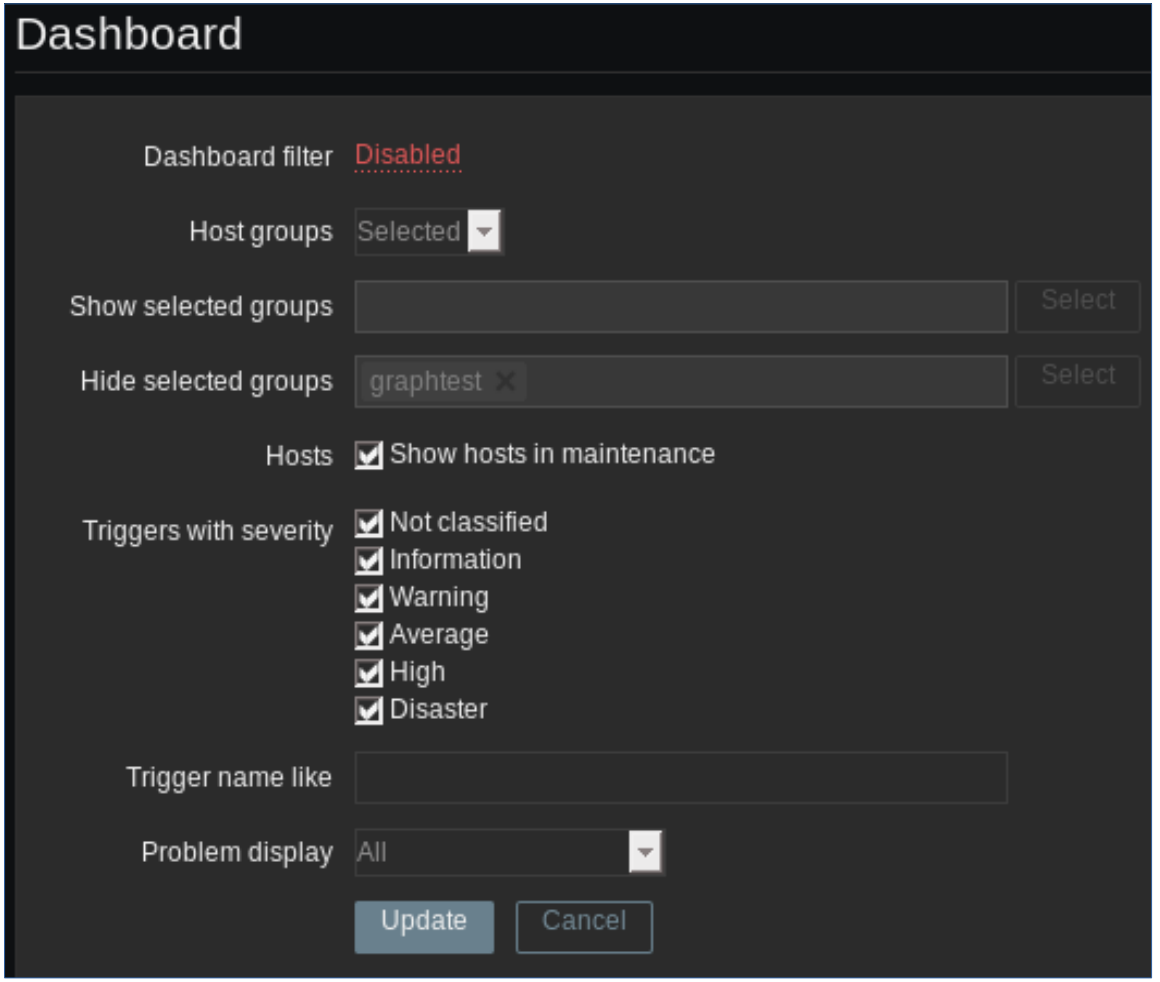
Filter the top 100



- Host/host group
- Severity
- Specific time period

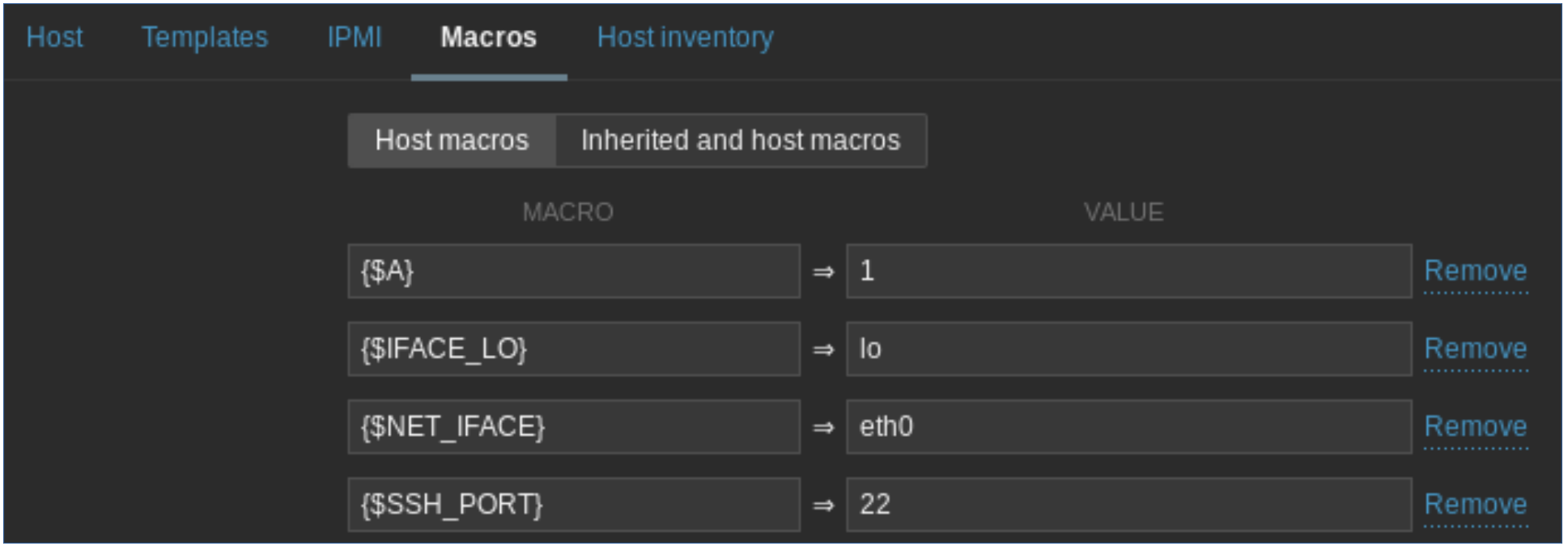
Zabbix 3.0
Frontend usability

Improved dashboard config – filter by trigger



Zabbix 3.0
Frontend usability

Macros resolve to...



Zabbix 3.0
Frontend usability

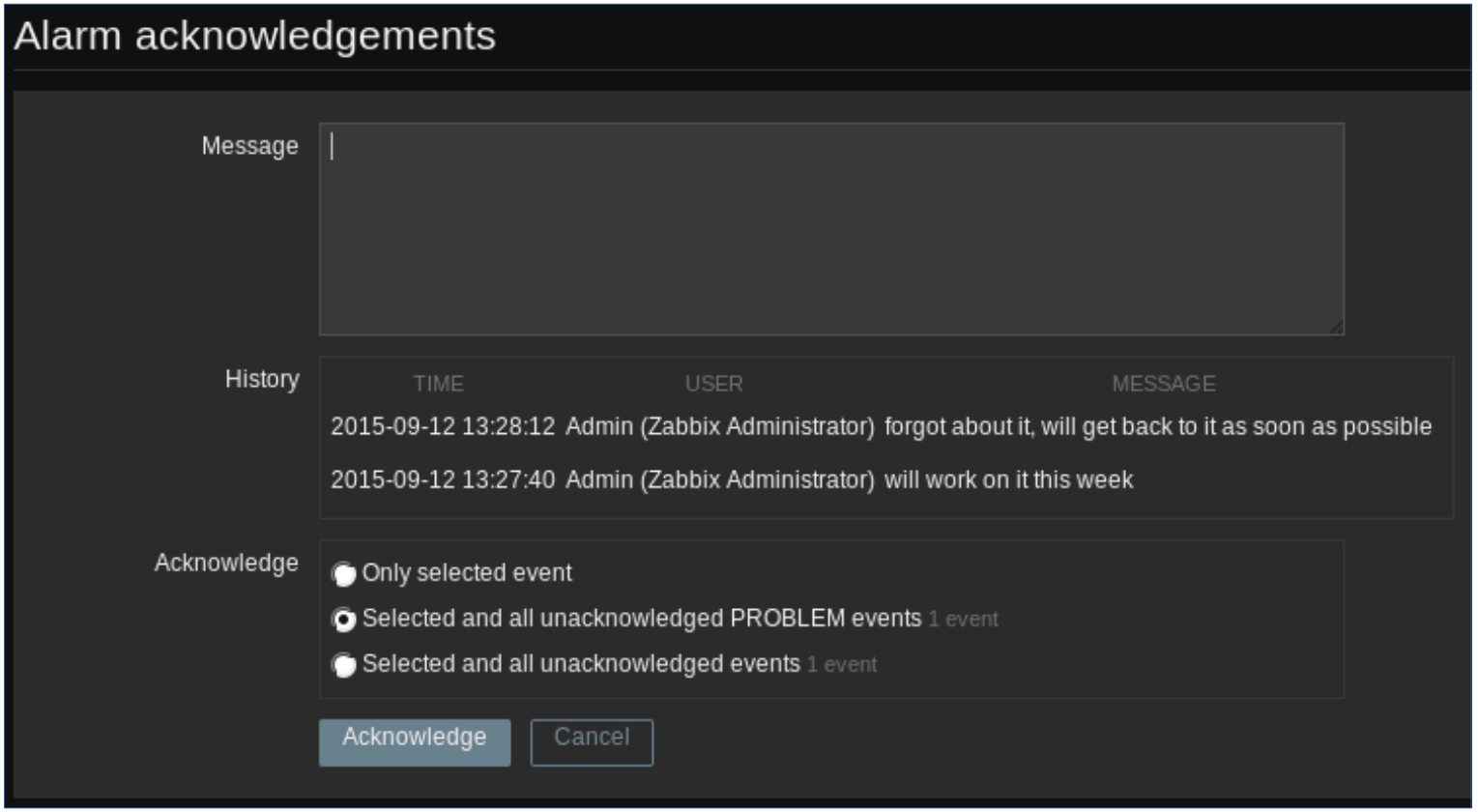
... on various level

Host macros | Inherited and host macros

MACRO		EFFECTIVE VALUE	TEMPLATE VALUE	GLOBAL VALUE (CONFIGURE)
{$A}	⇒	1	Remove ⇐ second_level: "13"	⇐ "234"
{$B}	⇒	123	Change	⇐ "123"
{$CPU_LOAD}	⇒	5	Change	⇐ "5"
{$IFACE_LO}	⇒	lo	Remove	
{$NET_IFACE}	⇒	eth0	Remove	
{$SECOND_LEVEL}	⇒	*\	Change ⇐ second_level: "*\"	
{$SSH_PORT}	⇒	22	Remove	⇐ "22"
{$TESTMACRO2}	⇒	testmacro2-template	Change ⇐ C_Template_Linux: "testmacro2-template"	

Zabbix 3.0
Frontend usability

Improved event acknowledging



Zabbix 3.0
Frontend usability

More power to standard user

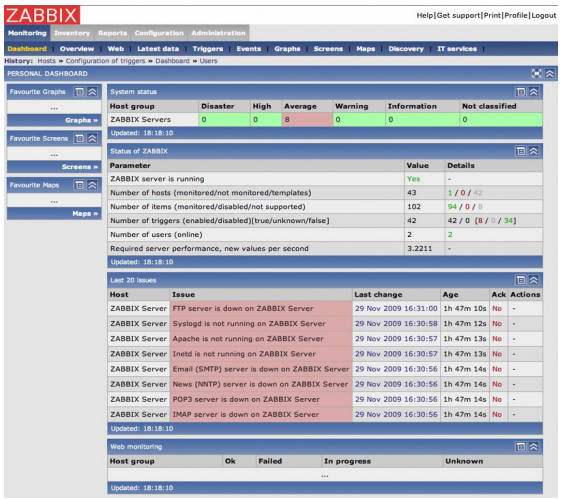
Maps, screens, slideshows:

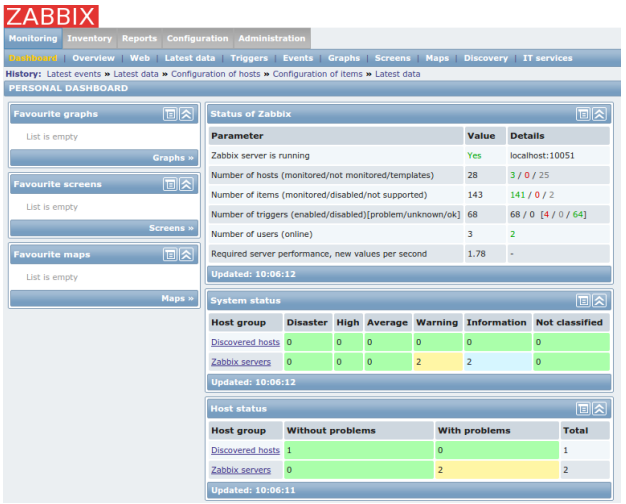
- User can create them
- User can share them

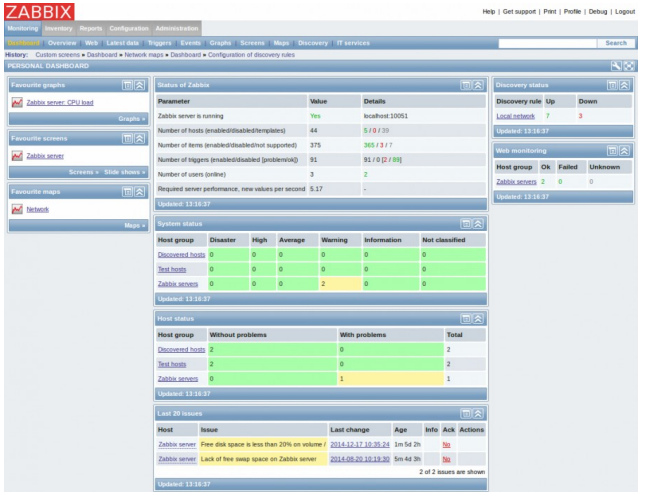
New design

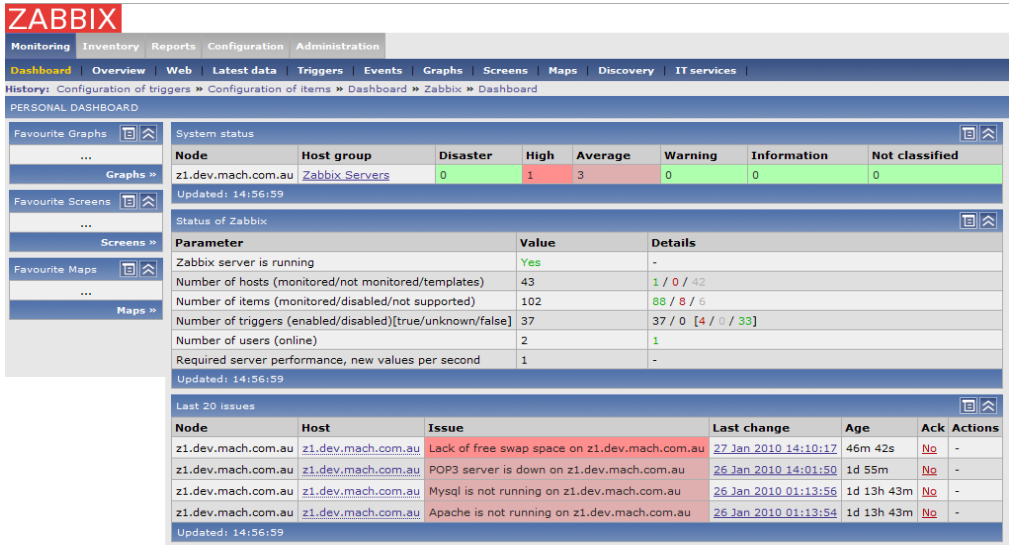
Zabbix 3.0
New Design

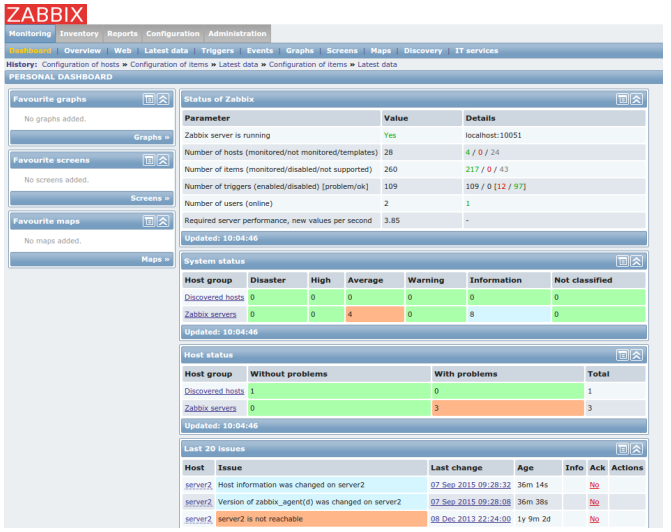
Zabbix 1.6 – 2.4





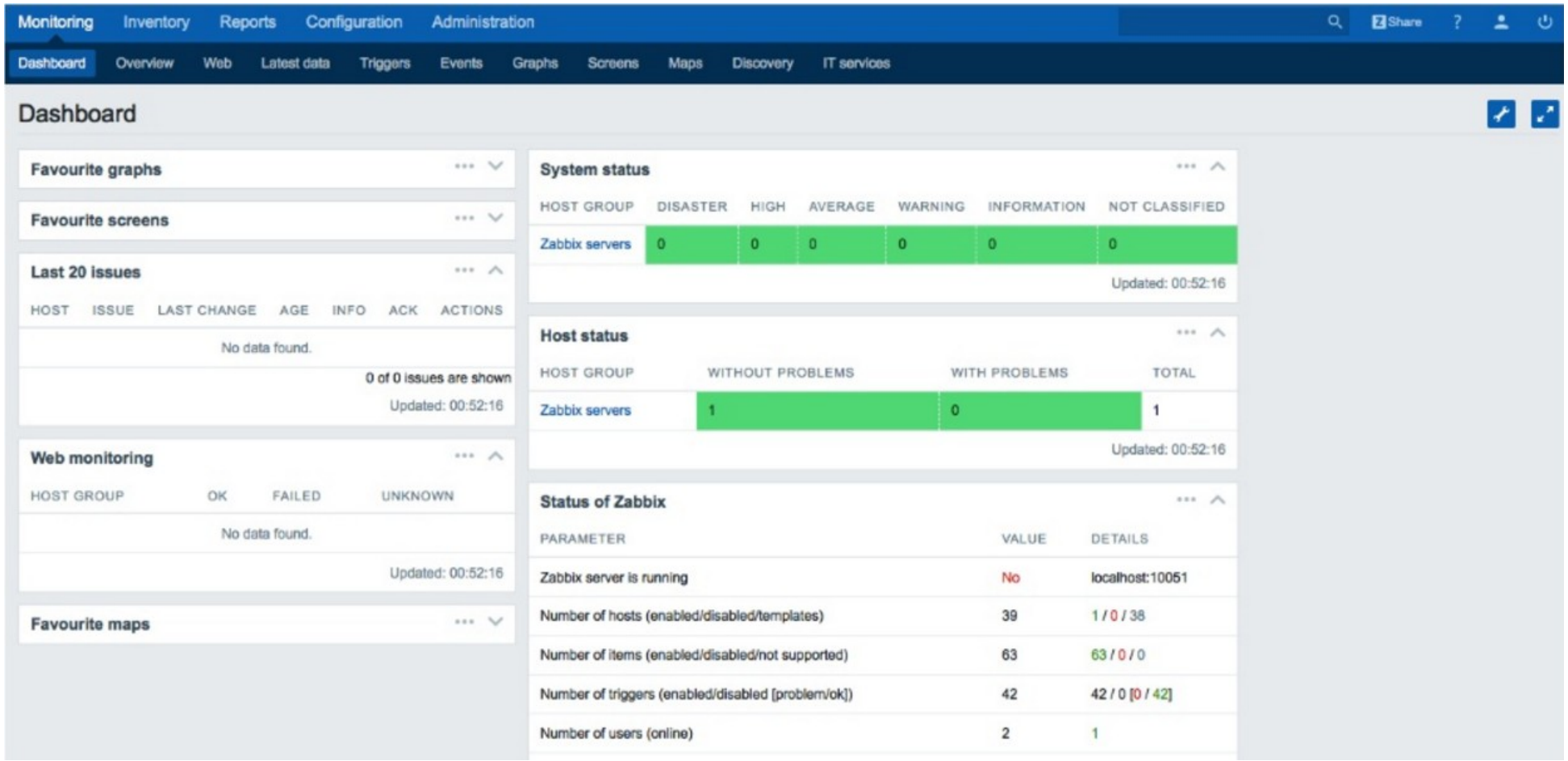






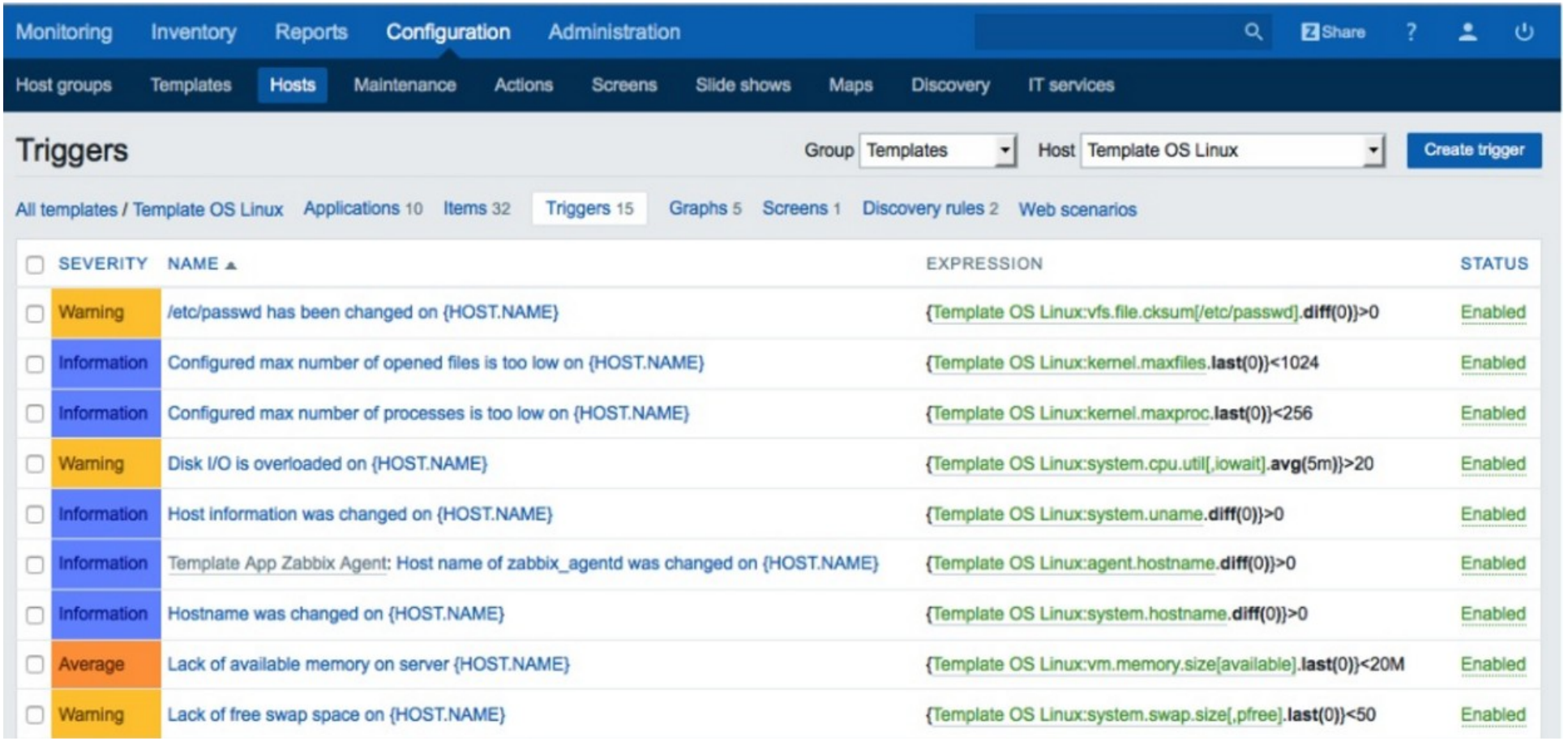
Zabbix 3.0 New Design

Zabbix 3.0



Zabbix 3.0 New Design

Zabbix 3.0



LLD
Low Level Discovery

Zabbix 3.0
LLD – Low Level Discovery

Multi OID SNMP Discovery

```
discovery[{#MACRO1}, oid1, {#MACRO2}, oid2, …]
```

Example: Discover ifDescr & ifAlias

```
{
    "data":[
      {"{#SNMPINDEX}":1,"{#IFDESCR}":"Interface #1","{#IFALIAS}":"eth1"},
      {"{#SNMPINDEX}":2,"{#IFDESCR}":"Interface #2","{#IFALIAS}":"eth2"},
      {"{#SNMPINDEX}":3,"{#IFALIAS}":"eth3"},
      {"{#SNMPINDEX}":4,"{#IFDESCR}":"Interface #4"},
      {"{#SNMPINDEX}":5,"{#IFALIAS}":"eth5"}
    ]
}
```

Zabbix 3.0
LLD – Low Level Discovery

Discover Windows services

```
service.discovery
```

- Return multiple macros
- Filter results

{#SERVICE.NAME}
{#SERVICE.DISPLAYNAME}
{#SERVICE.DESCRIPTION}
{#SERVICE.STATE}
{#SERVICE.STATENAME}
{#SERVICE.PATH}
{#SERVICE.USER}
{#SERVICE.STARTUP}
{#SERVICE.STARTUPNAME}

Zabbix 3.0
LLD – Low Level Discovery

Database ODBC - db.odbc.discover

```
+----------+--------+
| host     | count  |
+----------+--------+
| Japan 1  |      5 |
| Japan 2  |     12 |
| Latvia   |      3 |
+----------+--------+
```

Zabbix 3.0
LLD – Low Level Discovery

Advanced macros – Context based

```
/          - 10%
/home      - 20%
/var       - 15%

{$<MACRO>:<context>}

{$FSFREE}            = 10
{$FSFREE:/home}      = 20
{$FSFREE:/var}       = 15
```

Encryption

Zabbix 3.0 Encryption

Why would it be needed?

Encryption

- Protect sensitive data (e.g. configuration data from Zabbix server to proxy may contain credentials for accessing monitored hosts)

Authentication

- Trust a peer on “the other end”
- Prevent sending spoofed data to Zabbix

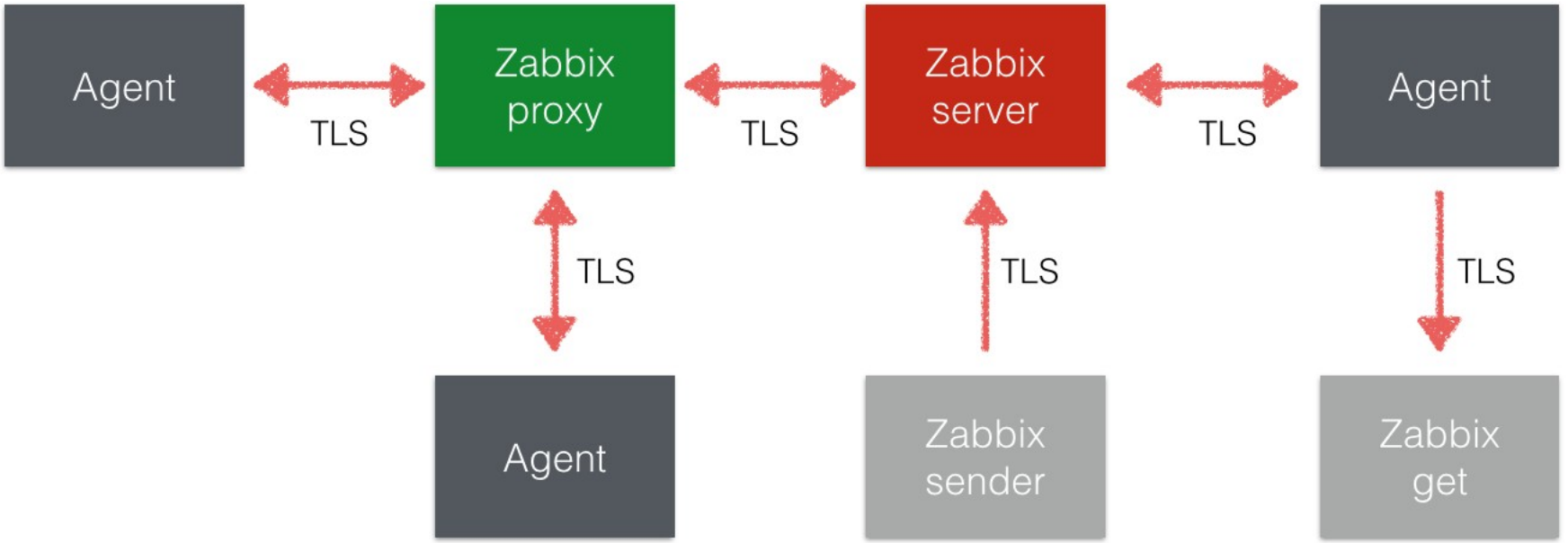
Zabbix 3.0 Encryption

Implementation

- OpenSSL, GnuTLS, or mbed TLS (PolarSSL) cryptographic toolkit can be used
- Different components can use different toolkits
- A connection can be configured to use a **certificate** or **PSK**
- Use the same ports as unencrypted
- Two parts: TO host (for passive checks) and FROM host (for active checks and zabbix_sender)

Zabbix 3.0 Encryption

All connections between Zabbix server, proxies and agents can be selectively configured to use encryption or stay unencrypted.



QA Time :-)

IntelliTrend IT-Services GmbH

Otto-Brenner-Strasse 119

D-33607 Bielefeld

Germany

Contact: Wolfgang Alper

Email: wolfgang.alper@intellitrend.de

www.intellitrend.de

Thank You!

For more information visit **www.zabbix.com**

IntelliTrend IT-Services GmbH

Otto-Brenner-Strasse 119

D-33607 Bielefeld

Germany

Contact: Wolfgang Alper

Email: wolfgang.alper@intellitrend.de

www.intellitrend.de