Welcome to Zabbix Conference 2016!
Who am I?

Alexei Vladishev
Creator of Zabbix
CEO, Architect and Product Manager
Twitter: @avladishev
Our sponsors
Conference stats
223 participants
223 participants from 38 countries
Top five countries

1. ........ 16
2. France 13
3. Netherlands 11
4. Lithuania 10
5. Germany 9

* excluding Latvia
Top five countries

1. **Russia 16**
2. France 13
3. Netherlands 11
4. Lithuania 10
5. Germany 9

* excluding Latvia
What’s happened in 2016
Release of Zabbix 3.0 LTS

Long Term Support (LTS) till 2021
Faster development, better support

45 people in Riga, Tokyo and New York
Last but not least...

Zabbix is a True Open Source software and will always be.
Let’s talk about Zabbix 3.2
Quick reminder

Zabbix 3.2 is the next major release, non LTS, 6-7 months support period
Event correlation
Example of a local event correlation
Log file monitoring

/var/log/services.log

...  
10/Aug/2016:06:25:30 service Jira stopped  
10/Aug/2016:06:25:32 service MySQL stopped  
10/Aug/2016:06:26:11 service MySQL started  
10/Aug/2016:06:26:22 service Redis stopped  
10/Aug/2016:06:26:58 service Redis started  
10/Aug/2016:06:27:31 service Jira started  
...

How many items and triggers we need to monitor state of each service and have independent notification?
Zabbix 3.2:

One item and one trigger to monitor all services!
<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Service {{ITEM.VALUE}}.repgsub(&quot;^.<em>service ([a-zA-Z]</em>) .*$&quot;, &quot;,1&quot;)} stopped</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Severity</strong></td>
<td>Not classified</td>
</tr>
<tr>
<td><strong>Problem expression</strong></td>
<td>{Template Services:log/[var/log/services].regexp(&quot;stopped&quot;)}=1</td>
</tr>
<tr>
<td><strong>Expression constructor</strong></td>
<td></td>
</tr>
<tr>
<td><strong>OK event generation</strong></td>
<td>Expression</td>
</tr>
<tr>
<td><strong>Recovery expression</strong></td>
<td>{Template Services:log/[var/log/services].regexp(&quot;started&quot;)}=1</td>
</tr>
<tr>
<td><strong>Expression constructor</strong></td>
<td></td>
</tr>
<tr>
<td><strong>PROBLEM event generation mode</strong></td>
<td>Single</td>
</tr>
<tr>
<td>Tags</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Datacenter</td>
<td>FR2</td>
</tr>
<tr>
<td>Env</td>
<td>Staging</td>
</tr>
<tr>
<td>Service</td>
<td>{{ITEM.VALUE}.regsub(&quot;.<em>service ([a-zA-Z]</em>).*&quot;, &quot;1&quot;)}</td>
</tr>
</tbody>
</table>

**PROBLEM event generation mode**
- Single
- Multiple

**OK event closes**
- All problems
- All problems if tag values match

**Tag for matching**
- Service

**Allow manual close**
- Yes
How will it work?

10/Aug/2016:06:25:30 service Jira stopped  “Service Jira stopped”  PROBLEM
How will it work?

10/Aug/2016:06:25:30 service Jira stopped
“Service Jira stopped” PROBLEM

10/Aug/2016:06:27:32 service MySQL stopped
“Service MySQL stopped” PROBLEM
How will it work?

10/Aug/2016:06:25:30 service Jira stopped
10/Aug/2016:06:27:32 service MySQL stopped
10/Aug/2016:06:28:11 service MySQL started

“Service Jira stopped”  PROBLEM
“Service MySQL stopped”  RESOLVED
How will it work?

10/Aug/2016:06:25:30 service Jira stopped
10/Aug/2016:06:27:32 service MySQL stopped
10/Aug/2016:06:28:11 service MySQL started
10/Aug/2016:06:34:22 service Redis stopped

“Service Jira stopped” PROBLEM
“Service MySQL stopped” RESOLVED
“Service Redis stopped” PROBLEM
How will it work?

10/Aug/2016:06:25:30 service Jira stopped
10/Aug/2016:06:27:32 service MySQL stopped
10/Aug/2016:06:28:11 service MySQL started
10/Aug/2016:06:34:22 service Redis stopped
10/Aug/2016:06:37:58 service Redis started

“Service Jira stopped” **PROBLEM**
“Service MySQL stopped” **RESOLVED**
“Service Redis stopped” **RESOLVED**
How will it work?

10/Aug/2016:06:25:30 service Jira stopped
“Service Jira stopped” RESOLVED
10/Aug/2016:06:27:32 service MySQL stopped
“Service MySQL stopped” RESOLVED
10/Aug/2016:06:28:11 service MySQL started
10/Aug/2016:06:34:22 service Redis stopped
“Service Redis stopped” RESOLVED
10/Aug/2016:06:37:58 service Redis started
10/Aug/2016:06:55:31 service Jira started
Tags give us ability to switch from host-to service-centric problem reporting and notifications
But it’s not limited only to services!
Different dimensions

Service: Oracle
Service: {ITEM.VALUE}.regsub(‘…’, ’1 \2’)

Datacenter: NY2
Datacenter: {$DATACENTER}

Area: Performance
Area: Availability
Area: Security

Environment: Staging
Environment: Test

User impact: None
User impact: Critical
So many problems
By environment: Production
By datacenter: NY2
By impact: Critical
By impact: Critical AND in NY2
Problem view
<table>
<thead>
<tr>
<th>Time</th>
<th>Severity</th>
<th>Recovery time</th>
<th>Status</th>
<th>Info</th>
<th>Host</th>
<th>Problem</th>
<th>Duration</th>
<th>Ack</th>
<th>Actions</th>
<th>Tags</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:01:46</td>
<td>Average</td>
<td></td>
<td></td>
<td></td>
<td>Linux009</td>
<td>Too many queries per second</td>
<td>1m 19s</td>
<td>Yes</td>
<td>In progress</td>
<td>Datacenter: NY1</td>
</tr>
<tr>
<td>15:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13:06:05</td>
<td>High</td>
<td></td>
<td></td>
<td></td>
<td>Linux005</td>
<td>Service Jira stopped</td>
<td>1h 57m 2s</td>
<td>No</td>
<td>Done 2</td>
<td>Datacenter: FR2</td>
</tr>
<tr>
<td>13:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:33:02</td>
<td>High</td>
<td></td>
<td></td>
<td></td>
<td>Linux005</td>
<td>Service Redis stopped</td>
<td>4h 30m 5s</td>
<td>No</td>
<td>Done 2</td>
<td>Datacenter: FR2</td>
</tr>
<tr>
<td>Today</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016-09-07 17:09:36</td>
<td>Information</td>
<td></td>
<td></td>
<td></td>
<td>Linux008</td>
<td>Low CPU utilization on host machines</td>
<td>21h 53m 29s</td>
<td>No</td>
<td></td>
<td>Datacenter: FR2</td>
</tr>
<tr>
<td>2016-09-07 09:58:08</td>
<td>Average</td>
<td></td>
<td></td>
<td></td>
<td>Linux001</td>
<td>Too many transactions per second</td>
<td>1d 5h 4m</td>
<td>Yes</td>
<td>Failures 1</td>
<td>Datacenter: FR2</td>
</tr>
<tr>
<td>Yesterday</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016-07-18 11:06:36</td>
<td>Warning</td>
<td></td>
<td></td>
<td></td>
<td>Linux002</td>
<td>Too many processes running on Linux002</td>
<td>1m 22d 3h</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016-07-18 11:06:38</td>
<td>Warning</td>
<td></td>
<td></td>
<td></td>
<td>Linux007</td>
<td>Too many processes running on Linux007</td>
<td>1m 22d 3h</td>
<td>Yes</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2016-07-18 11:06:26</td>
<td>Warning</td>
<td></td>
<td></td>
<td></td>
<td>Linux001</td>
<td>Too many processes running on Linux001</td>
<td>1m 22d 3h</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016-07-18 11:06:14</td>
<td>Warning</td>
<td></td>
<td></td>
<td></td>
<td>Linux010</td>
<td>Too many processes running on Linux010</td>
<td>1m 22d 3h</td>
<td>No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Filtering!
<table>
<thead>
<tr>
<th>Time</th>
<th>Status</th>
<th>Info</th>
<th>Host</th>
<th>Problem</th>
<th>Duration</th>
<th>Ack</th>
<th>Actions</th>
<th>Tags</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:06:56</td>
<td>PROBLEM</td>
<td></td>
<td>Linux009</td>
<td>Too many queries per second</td>
<td>1s</td>
<td>No</td>
<td></td>
<td>Datacenter: NY1, Env: Production, Service: HTTP balancer</td>
</tr>
<tr>
<td>15:01:49</td>
<td>RESOLVED</td>
<td>15:06:49</td>
<td>Linux009</td>
<td>Too many queries per second</td>
<td>5m 1s</td>
<td>Yes</td>
<td>1</td>
<td>Datacenter: NY1, Env: Production, Service: HTTP balancer</td>
</tr>
</tbody>
</table>
Notifications
**Actions**

**Name**: Critical problems with production load balancer

**Type of calculation**: And

<table>
<thead>
<tr>
<th>Conditions</th>
<th>Label</th>
<th>Name</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
<td>Tag Service = HTTP balancer</td>
<td>Remove</td>
</tr>
<tr>
<td></td>
<td>B</td>
<td>Tag Impact = Critical</td>
<td>Remove</td>
</tr>
<tr>
<td></td>
<td>C</td>
<td>Tag Env = Production</td>
<td>Remove</td>
</tr>
</tbody>
</table>

**New condition**

- **Trigger name**: like

**Enabled**: ✔️

**Buttons**: Update, Clone, Delete, Cancel
Global correlation
Existing problems

Correlation rules

New problem comes

?
Existing problems

No correlation found

Correlation rules
Existing problems

Close older problems

Correlation rules
Existing problems

New problem will be closed immediately

Correlation rules
Event correlation rules

Correlation

Name: Correlate network port problems
Type of calculation: And/Or

Conditions:

<table>
<thead>
<tr>
<th>Label</th>
<th>Name</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Old event tag Port = new event tag Port</td>
<td>Remove</td>
</tr>
<tr>
<td>B</td>
<td>Old event tag Host = new event tag Host</td>
<td>Remove</td>
</tr>
</tbody>
</table>

New condition:

Old event tag Port = tag

Description:

Keep only one problem per network port.

Enabled: On

Actions:

Update  Clone  Delete  Cancel
### Event correlation rules

<table>
<thead>
<tr>
<th>Correlation</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operations</strong></td>
<td>Details</td>
</tr>
<tr>
<td>Close new event</td>
<td></td>
</tr>
<tr>
<td>New operation</td>
<td>Close old events</td>
</tr>
<tr>
<td></td>
<td>Add</td>
</tr>
</tbody>
</table>

**Actions:**
- Update
- Clone
- Delete
- Cancel
Problem tags and correlation is a solid foundation for further improvements.
### Nested host groups

<table>
<thead>
<tr>
<th>Servers</th>
<th>Location/Africa</th>
<th>Location/Europe</th>
<th>Location/Japan</th>
<th>Location/North America</th>
<th>Templates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Servers/Physical</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Templates/Official</td>
</tr>
<tr>
<td>Servers/VMs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Templates/SNMP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Templates/Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Templates/Vendors</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Templates/Vendors/HP</td>
</tr>
</tbody>
</table>
Redesigned permissions
Filtering
Manually close problems
Event acknowledgements

Message: There was a problem with version of MySQL in production. Updated, restarted, should be fine now.

History:

<table>
<thead>
<tr>
<th>Time</th>
<th>User</th>
<th>Message</th>
<th>User action</th>
</tr>
</thead>
</table>

Acknowledge:
- Only selected problem
- Selected and all other unacknowledged problems of related triggers (6 events)

Close problem: ☑

[Acknowledgment button] [Cancel button]
<table>
<thead>
<tr>
<th>Time</th>
<th>Severity</th>
<th>Recovery time</th>
<th>Status</th>
<th>Info</th>
<th>Host</th>
<th>Problem</th>
<th>Duration</th>
<th>Ack</th>
<th>Actions</th>
<th>Tags</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:06:56</td>
<td>Average</td>
<td></td>
<td></td>
<td></td>
<td>Linux009</td>
<td>Too many queries per second</td>
<td>8h 50m 10s</td>
<td>No</td>
<td>Done</td>
<td>Datacenter: NY1</td>
</tr>
<tr>
<td>15:00:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13:06:05</td>
<td>High</td>
<td>23:57:00</td>
<td>RESOLVED</td>
<td></td>
<td>Linux005</td>
<td>Service Jira stopped</td>
<td>10h 50m 55s</td>
<td>Yes</td>
<td>In progress</td>
<td>Datacenter: FR2</td>
</tr>
<tr>
<td>13:00:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:33:02</td>
<td>High</td>
<td></td>
<td></td>
<td></td>
<td>Linux005</td>
<td>Service Redis stopped</td>
<td>13h 24m 4s</td>
<td>No</td>
<td>Done</td>
<td>Datacenter: FR2</td>
</tr>
<tr>
<td>Today</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016-09-07</td>
<td>Information</td>
<td></td>
<td></td>
<td></td>
<td>Linux008</td>
<td>Low CPU utilization on host machines</td>
<td>1d 6h 47m</td>
<td>No</td>
<td></td>
<td>Datacenter: FR2</td>
</tr>
</tbody>
</table>

Resolved by user "Admin (Zabbix Administrator)".

Datacenter: NY1, Env: Production, Service: HTTP balancer

Datacenter: FR2, Env: Staging, Service: Jira

Datacenter: FR2, Env: Staging, Service: Redis

Datacenter: FR2, Service: Kubernetes
Trigger hysteresis? Easy!
Trigger Dependencies

Name: Too many queries per second
Severity: Average

Problem expression: \{Template Services: http.qps.avg(1m)\}>5000

OK event generation:
- Expression: None
- Recovery expression: \{Template Services: http.qps.avg(5m)\}<1000

Recovery expression: 

Expression constructor
Viewable items, triggers, graphs created by LLD
### Items

<table>
<thead>
<tr>
<th>Mounted filesystem discovery: Free disk space on /</th>
<th>vfs.fs.size[/,free]</th>
<th>1m</th>
<th>7d</th>
<th>365d</th>
<th>Zabbix agent</th>
<th>Filesystems</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mounted filesystem discovery: Free disk space on /boot</td>
<td>vfs.fs.size[/boot,free]</td>
<td>1m</td>
<td>7d</td>
<td>365d</td>
<td>Zabbix agent</td>
<td>Filesystems</td>
<td>Enabled</td>
</tr>
<tr>
<td>Mounted filesystem discovery: Free disk space on / (percentage)</td>
<td>vfs.fs.size[/,pfree]</td>
<td>1m</td>
<td>7d</td>
<td>365d</td>
<td>Zabbix agent</td>
<td>Filesystems</td>
<td>Enabled</td>
</tr>
<tr>
<td>Mounted filesystem discovery: Free disk space on /boot (percentage)</td>
<td>vfs.fs.size[/boot,pfree]</td>
<td>1m</td>
<td>7d</td>
<td>365d</td>
<td>Zabbix agent</td>
<td>Filesystems</td>
<td>Enabled</td>
</tr>
<tr>
<td>Mounted filesystem discovery: Free inodes on / (percentage)</td>
<td>vfs.fs.inode[/,pfree]</td>
<td>1m</td>
<td>7d</td>
<td>365d</td>
<td>Zabbix agent</td>
<td>Filesystems</td>
<td>Enabled</td>
</tr>
<tr>
<td>Mounted filesystem discovery: Free inodes on /boot (percentage)</td>
<td>vfs.fs.inode[/boot,pfree]</td>
<td>1m</td>
<td>7d</td>
<td>365d</td>
<td>Zabbix agent</td>
<td>Filesystems</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

### Triggers

<table>
<thead>
<tr>
<th>Warning</th>
<th>Mounted filesystem discovery: Free disk space is less than 20% on volume /</th>
<th>{Linux001:vfs.fs.size[/,pfree].last(0)&lt;20}</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warning</td>
<td>Mounted filesystem discovery: Free disk space is less than 20% on volume /boot</td>
<td>{Linux001:vfs.fs.size[/boot,pfree].last(0)&lt;20}</td>
<td>Enabled</td>
</tr>
<tr>
<td>Warning</td>
<td>Mounted filesystem discovery: Free inodes is less than 20% on volume /</td>
<td>{Linux001:vfs.fs.inode[/,pfree].last(0)&lt;20}</td>
<td>Enabled</td>
</tr>
<tr>
<td>Warning</td>
<td>Mounted filesystem discovery: Free inodes is less than 20% on volume /boot</td>
<td>{Linux001:vfs.fs.inode[/boot,pfree].last(0)&lt;20}</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
Better actions and escalations
### Actions

<table>
<thead>
<tr>
<th>Operation</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Send message to users</strong>: Alexei Vladishev via all media</td>
</tr>
<tr>
<td>2</td>
<td><strong>Run remote commands on current host</strong></td>
</tr>
</tbody>
</table>

**Default operation step duration**: 60 (minimum 60 seconds)

**Default subject**: `{TRIGGER.STATUS}: {TRIGGER.NAME}`

**Default message**:
- Trigger: `{TRIGGER.NAME}`
- Trigger status: `{TRIGGER.STATUS}`
- Trigger severity: `{TRIGGER.SEVERITY}`
- Trigger URL: `{TRIGGER.URL}`

Pause operations while in maintenance: **on**
### Actions

#### Recovery operations

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default subject</td>
<td>{TRIGGER.STATUS}: {TRIGGER.NAME}</td>
</tr>
</tbody>
</table>
| Default message| Trigger: {TRIGGER.NAME}  
|                | Trigger status: {TRIGGER.STATUS}  
|                | Trigger severity: {TRIGGER.SEVERITY}  
|                | Trigger URL: {TRIGGER.URL}  
| Item values    | |

<table>
<thead>
<tr>
<th>Operations</th>
<th>Details</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details</td>
<td><strong>Send message to users:</strong> alex (Alexei Vladishev) via all media</td>
<td></td>
</tr>
<tr>
<td>New</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action Button</th>
<th>Update</th>
<th>Clone</th>
<th>Delete</th>
<th>Cancel</th>
</tr>
</thead>
</table>
Also...

Web scenario export/import
Function evaluation for NOTSUPPORTED items
Coping with fast-growing log files
Support of regex in count ()
and much more!
For detailed list of new features see

Documentation of Zabbix 3.2
Zabbix 3.2 is a result of active cooperation with our partners and customers.

Special thanks to S&T Slovakia s.r.o.
How to upgrade?
Nothing special, except …

Some history tables are affected: `history_log`, `history_text`

It may take time to execute depending on size of log and text data stored in the database
Where is Zabbix 3.2?
Zabbix 3.2.0 is expected to be released very soon
Enjoy the conference!

Thanks for your support