Supercharge Zabbix with Powerful Insights

Aleksandrs Kalimulins, C Developer, Zabbix, Latvia
KINDS OF MONITORING

☑️ Compare values to known thresholds

{Host:cpu.temp.avg(5m)} > 100
IT DEPENDS...
WEB TRAFFIC MONITORING
KINDS OF MONITORING

ZABBIX: ALL YOUR BASELINE ARE BELONG TO US
KINDS OF MONITORING

✔️ Compare values to known thresholds

{Host:cpu.temp.avg(5m)} > 100

✔️ Baseline – compare to unknown thresholds
WEB TRAFFIC MONITORING
WEB TRAFFIC MONITORING

September, 2019

September, 2020
ZABBIX 5.0

* Expression

```
{shop.example.com:traffic.data.avg(30d)} >
{shop.example.com:traffic.data.avg(30d,365d)} *
{$GROWTH_FACTOR}
```
ZABBIX 5.0

Expression

\{shop.example.com:traffic.data.avg(30d)\} > \{shop.example.com:traffic.data.avg(30d, 365d)\} \times \{$GROWTH\_FACTOR$\}

Expression constructor

Trigger status (the expression) is recalculated every time Zabbix server receives a new value that is part of the expression.

Triggers are evaluated based on history data only; trend data are never considered.

If time-based functions (nodata(), date(), dayofmonth(), dayofweek(), time(), now()) are in the expression, the trigger is recalculated every 30 seconds by a Zabbix history syncer.
ZABBIX 5.0

- 30d and 365d are just 187200 and 68328000 seconds
- \texttt{avg()} depends on time of calculation
ZABBIX 5.2 - NEW FUNCTIONS

trendavg(period, period_shift)
trendcount(period, period_shift)
trenddelta(period, period_shift)
trendmax(period, period_shift)
trendmin(period, period_shift)
trendsum(period, period_shift)
ZABBIX 5.2 - NEW FUNCTIONS

☑ Use trends tables instead of history
  
  • Don’t forget to set:
  
      Trends
      Enable internal housekeeping ☑
      Override item trend period ☑
      Data storage period 3650d

☑ Use Gregorian calendar for period and period_shift
  
  • h (hour), d (day), w (week), M (month) and y (year)

☑ Calculate upon the end of a period
ZABBIX 5.2 - NEW FUNCTIONS

• Customized event name:
  • New field in trigger definition
  • Optional, can use trigger Name instead
  • Use to display problem with a context
  • New macro `{? \ldots }` (“Expression macro”)

# ZABBIX 5.2 - NEW FUNCTIONS

## Triggers

<table>
<thead>
<tr>
<th>Trigger</th>
<th>Tags</th>
<th>Dependencies</th>
</tr>
</thead>
</table>

**Name**: Abnormal traffic on `{HOST.HOST}`

**Event name**: Abnormal traffic on `{HOST.HOST}`, exceeded by `{((HOST.HOST).traffic.data.trendavg(1M,now/M)) / ((HOST.HOST).traffic.data.trendavg(1M,now/M-1y) -1)*100}%`

**Operational data**

<table>
<thead>
<tr>
<th>Severity</th>
<th>Not classified</th>
<th>Information</th>
<th>Warning</th>
<th>Average</th>
<th>High</th>
<th>Disaster</th>
</tr>
</thead>
</table>

**Expression**: `{shop.example.com:traffic.data.trendavg(1M,now/M}) > \{shop.example.com:traffic.data.trendavg(1M,now/M-1y}\} \times \{\$ABNORMALITY_FACTOR\}`
ZABBIX 5.2 - NEW FUNCTIONS

### Triggers

<table>
<thead>
<tr>
<th>Trigger</th>
<th>Tags</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Abnormal traffic on {HOST.HOST}</td>
<td></td>
</tr>
<tr>
<td><strong>Event name</strong></td>
<td>Abnormal traffic on {HOST.HOST}, exceeded by ?{{HOST.HOST}:traffic.data.trendavg(1M,now/M)} / {{HOST.HOST}:traffic.data.trendavg(1M,now/M-1y)} -1*100%</td>
<td></td>
</tr>
<tr>
<td><strong>Operational data</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td>Not classified</td>
<td>Information</td>
</tr>
<tr>
<td><strong>Expression</strong></td>
<td>{shop.example.com:traffic.data.trendavg(1M,now/M)} &gt; {shop.example.com:traffic.data.trendavg(1M,now/M-1y)} * {$ABNORMALITY_FACTOR}</td>
<td></td>
</tr>
</tbody>
</table>

Expression constructor
# Zabbix 5.2 - New Functions

## Problems

<table>
<thead>
<tr>
<th>Time</th>
<th>Info</th>
<th>Host</th>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:14:17</td>
<td>shop.example.com</td>
<td>Abnormal traffic on shop.example.com, exceeded by 14.851131675138941%</td>
<td></td>
</tr>
</tbody>
</table>
ZABBIX 5.2 - NEW FUNCTIONS

- `fmtnum(digits)`
  - applicable to `ITEM.VALUE`, `ITEM.LASTVALUE` and expression macros
  - `fmtnum(2)` gives `14.85` instead of `14.8512345`

- `fmttime(format, time_shift)`
  - applicable to `{TIME}`
  - uses strftime format codes
  - `{TIME}.fmttime("%B,%Y")` gives October,2020
ZABBIX 5.2 - NEW FUNCTIONS

Triggers

**Name**
Abnormal traffic on `HOST.HOST`

**Event name**
Abnormal traffic on `HOST.HOST`, exceeded by `(((HOST.HOST):traffic.data.trendavg(1M,now/M)) / ((HOST.HOST):traffic.data.trendavg(1M,now/M-1y)} -1) * 100).fmtnum(2)%` (compared to `{TIME}.fmttime("%D,%Y","-13M")`)

**Operational data**

**Severity**
Not classified  Information  Warning  Average  High  Disaster

**Expression**
```
{shop.example.com:traffic.data.trendavg(1M,now/M)} >
{shop.example.com:traffic.data.trendavg(1M,now/M-1y)} *
{S$ABNORMALITY_FACTOR}
```
# ZABBIX 5.2 - NEW FUNCTIONS

<table>
<thead>
<tr>
<th>Time</th>
<th>Info</th>
<th>Host</th>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:14:17</td>
<td>shop.example.com</td>
<td></td>
<td>Abnormal traffic on shop.example.com, exceeded by 14.851131675138941%</td>
</tr>
</tbody>
</table>
CLOUD BUDGET MONITORING
CLOUD BUDGET MONITORING

• Set period_shift to future to calculate current month
  • trendsum(1M,now/M+1M)
• Use calculated items to calculate current periods
CLOUD BUDGET MONITORING
CLOUD BUDGET MONITORING

Items

All hosts / reports.example.com Enabled ZBX SNMP JMX IPMI Applications 2 Items 3 Triggers 1

<table>
<thead>
<tr>
<th>Item</th>
<th>Preprocessing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Current cloud monthly cost</td>
</tr>
<tr>
<td>Type</td>
<td>Calculated</td>
</tr>
<tr>
<td>Key</td>
<td>current.monthly.cost</td>
</tr>
<tr>
<td>Formula</td>
<td>trendsum(&quot;report.data&quot;,1M,now/M+1M)</td>
</tr>
<tr>
<td>Type of information</td>
<td>Numeric (float)</td>
</tr>
<tr>
<td>Units</td>
<td>$</td>
</tr>
<tr>
<td>Update interval</td>
<td>1d</td>
</tr>
</tbody>
</table>
# Cloud Budget Monitoring

<table>
<thead>
<tr>
<th>Trigger</th>
<th>Tags</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Monthly cloud budget exceeded</td>
<td></td>
</tr>
<tr>
<td><strong>Event name</strong></td>
<td>Monthly cloud budget exceeded on {HOST.HOST} by $({{HOST.HOST}:current.monthly.cost.last()} - {{MONTHLY_BUDGET}}).fmtnum(2)}</td>
<td></td>
</tr>
<tr>
<td><strong>Operational data</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td>Not classified</td>
<td>Information</td>
</tr>
<tr>
<td><strong>Expression</strong></td>
<td>{reports.example.com:current.monthly.cost.last()} &gt; {{MONTHLY_BUDGET}}</td>
<td></td>
</tr>
</tbody>
</table>
USE CASES

• Use trend functions for IT metrics and non-IT KPIs
• Real world applications:
  • Business performance
  • Sales and marketing
  • Warehousing
  • Human resources
  • Customer support
IN A NUTSHELL

- Analyze history without storing historical data
- Calendar hours days, weeks, months, years
- Trigger field Event name – events with context
- New formatting functions
- Long term data analysis better with Zabbix 5.2
Thank You!