ZABBIX

Tips and tricks for optimizing problem detection with Zabbix

Victor Credidio

Support Engineer and Certified Trainer

HOW ARE PROBLEMS DETECTED ON ZABBIX?

Zabbix is constantly collecting metrics from Hosts

- The values are collected by items (where most of them consider an update interval between collections)
- Any collected value can be evaluated againts a logical expression that will inform you if there is a problem
- These expressions are known as Triggers
  - ✓ If the Trigger expression is TRUE = PROBLEM
  - ✓ If the Trigger expression is FALSE = OK

Memory utilization > 90%

TRIGGERS IN MORE DETAILS

How does a trigger expression looks like?

- Syntax:

function(/host/key,<additional parameters>)<operator><constant>

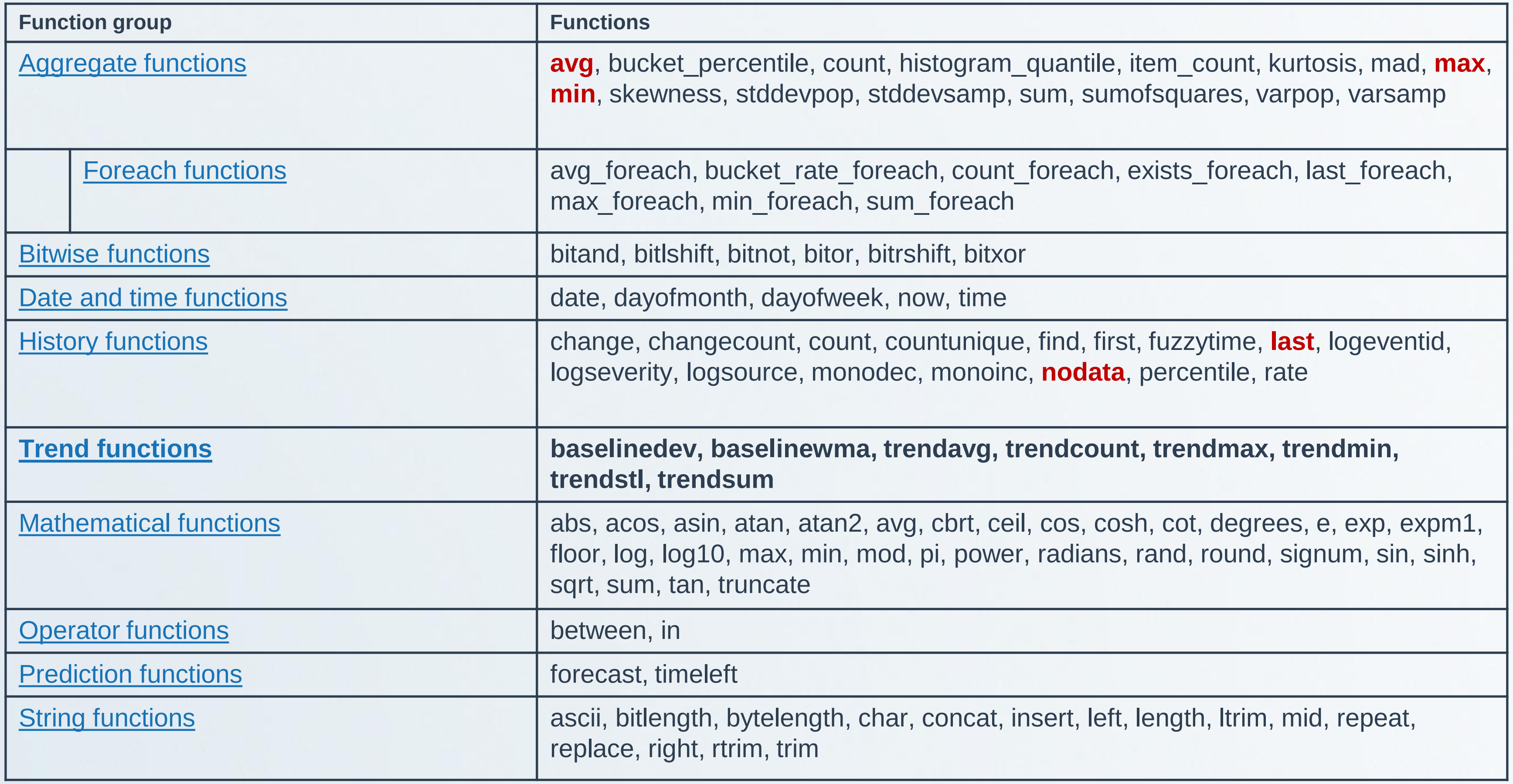
- ✓ **function**: allow to calculate the collected values (average, minimum, maximum, sum), find strings, reference current time and other factors. Depending on the Function, it will require some **additional parameters**.
- ✓ **host** and **key** **must exist** in Zabbix.
- ✓ An **<operator>** will be used to compare the result of the function with the **constant**.
- ✓ **constant** is the expected threshold/reference to define the expression state.

avg(/Production server/vm.memory.utilization[pused],5m)>90

TRIGGERS IN MORE DETAILS

Functions: the magic behind the triggers

- Available functions on Zabbix:

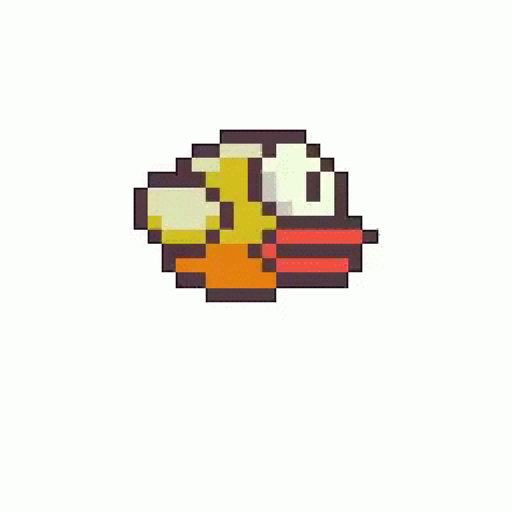


Function group	Functions
Aggregate functions	**avg**, bucket_percentile, count, histogram_quantile, item_count, kurtosis, mad, **max**, **min**, skewness, stddevpop, stddevsamp, sum, sumofsquares, varpop, varsamp
Foreach functions	avg_foreach, bucket_rate_foreach, count_foreach, exists_foreach, last_foreach, max_foreach, min_foreach, sum_foreach
Bitwise functions	bitand, bitlshift, bitnot, bitor, bitrshift, bitxor
Date and time functions	date, dayofmonth, dayofweek, now, time
History functions	change, changecount, count, countunique, find, first, fuzzytime, **last**, logeventid, logseverity, logsource, monodec, monoinc, **nodata**, percentile, rate
Trend functions	**baselinedev, baselinewma, trendavg, trendcount, trendmax, trendmin, trendstl, trendsum**
Mathematical functions	abs, acos, asin, atan, atan2, avg, cbrt, ceil, cos, cosh, cot, degrees, e, exp, expm1, floor, log, log10, max, min, mod, pi, power, radians, rand, round, signum, sin, sinh, sqrt, sum, tan, truncate
Operator functions	between, in
Prediction functions	forecast, timeleft
String functions	ascii, bitlength, bytelength, char, concat, insert, left, length, ltrim, mid, repeat, replace, right, rtrim, trim

COMMON MISTAKES AND RECOMMENDATIONS

Flapping:

- Really sensitive triggers can cause flapping

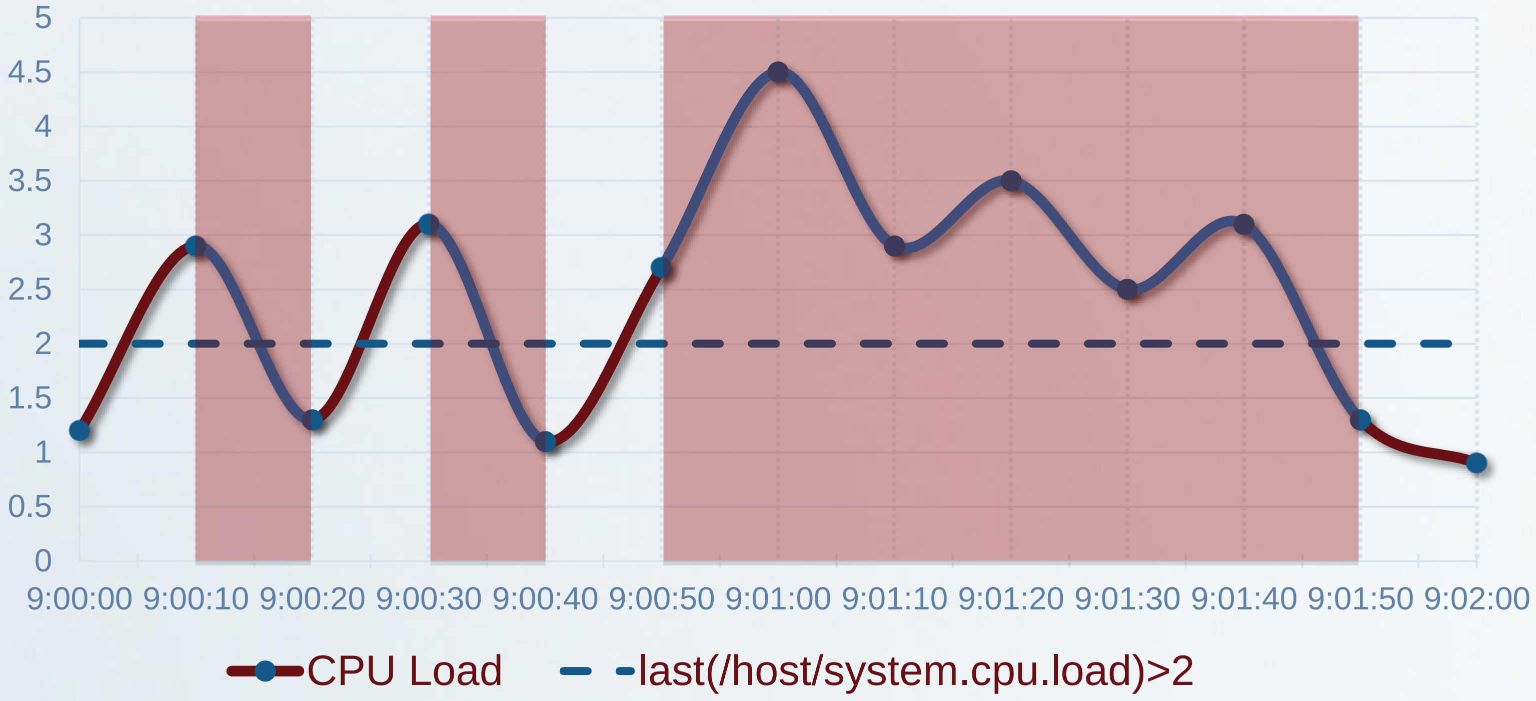


COMMON MISTAKES AND RECOMMENDATIONS

ZABBIX

Flapping:

- Really sensitive triggers can cause flapping

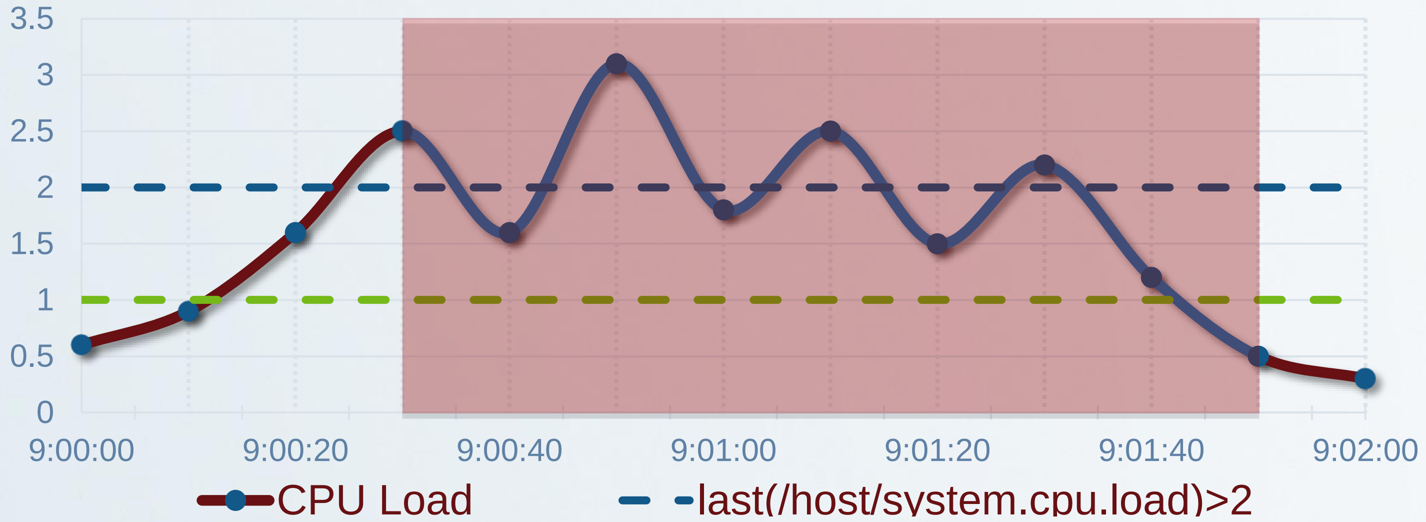


COMMON MISTAKES AND RECOMMENDATIONS

The last() function

- Can be really sensitive and lead to flapping
- Recommended the use of Recovery Expressions
  - ✓ Once a problem is detected, a different expression is used for recovery
  - ✓ When using a Recovery expression, the problem will recover if:

The trigger expression = **FALSE** and The recovery expression = **TRUE**



COMMON MISTAKES AND RECOMMENDATIONS

Additional note on the last() function

- Time period is not supported
- Using the # symbol will denote the Nth previous value

last(/host/key,#1) → Last value

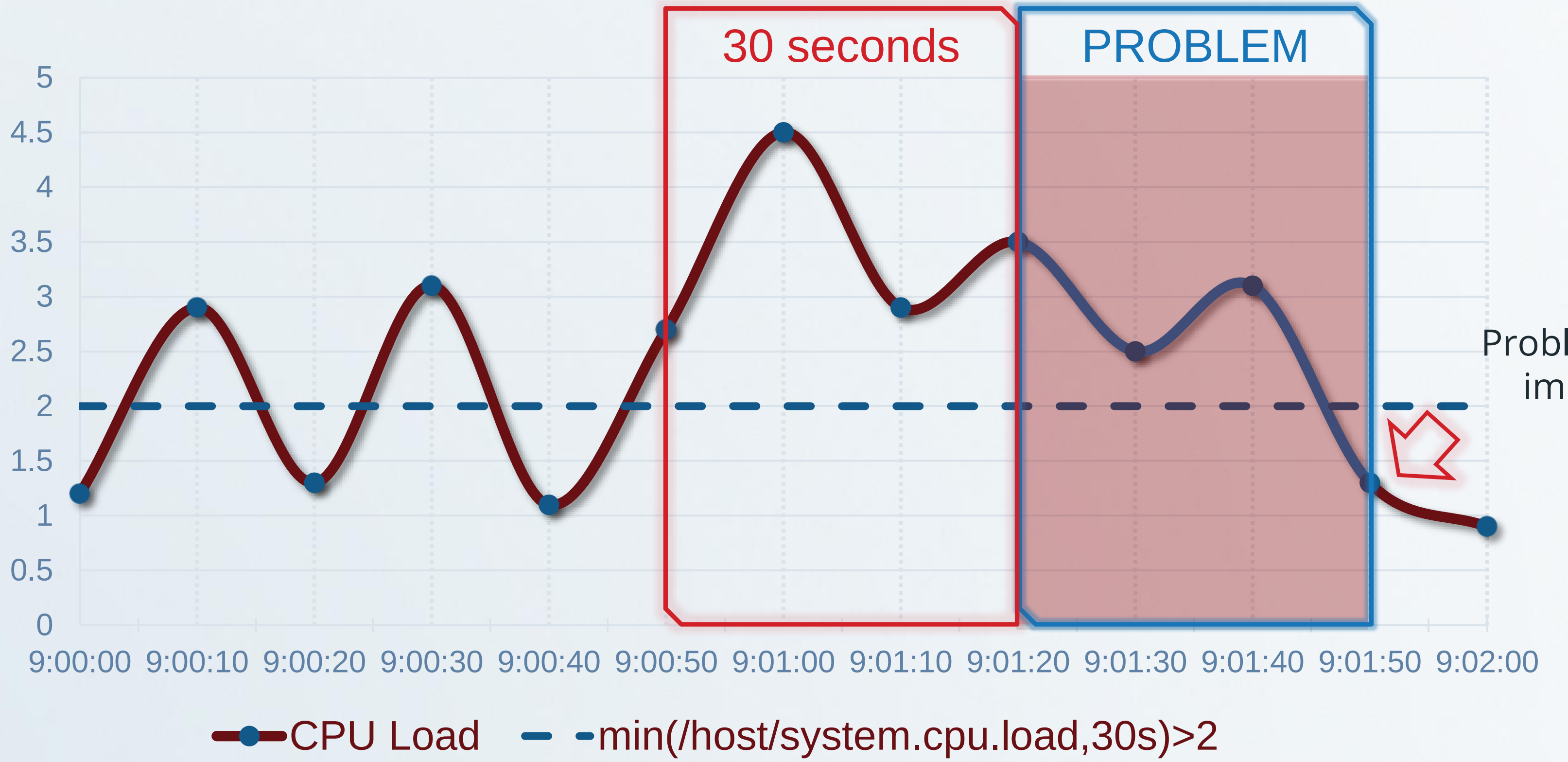
last(/host/key,#3) → 3rd previous value

last(/host/key,#3) and last(/host/key,#2) and last(/host/key)

COMMON MISTAKES AND RECOMMENDATIONS

The min() function

- Lowest value of an item within the defined evaluation period



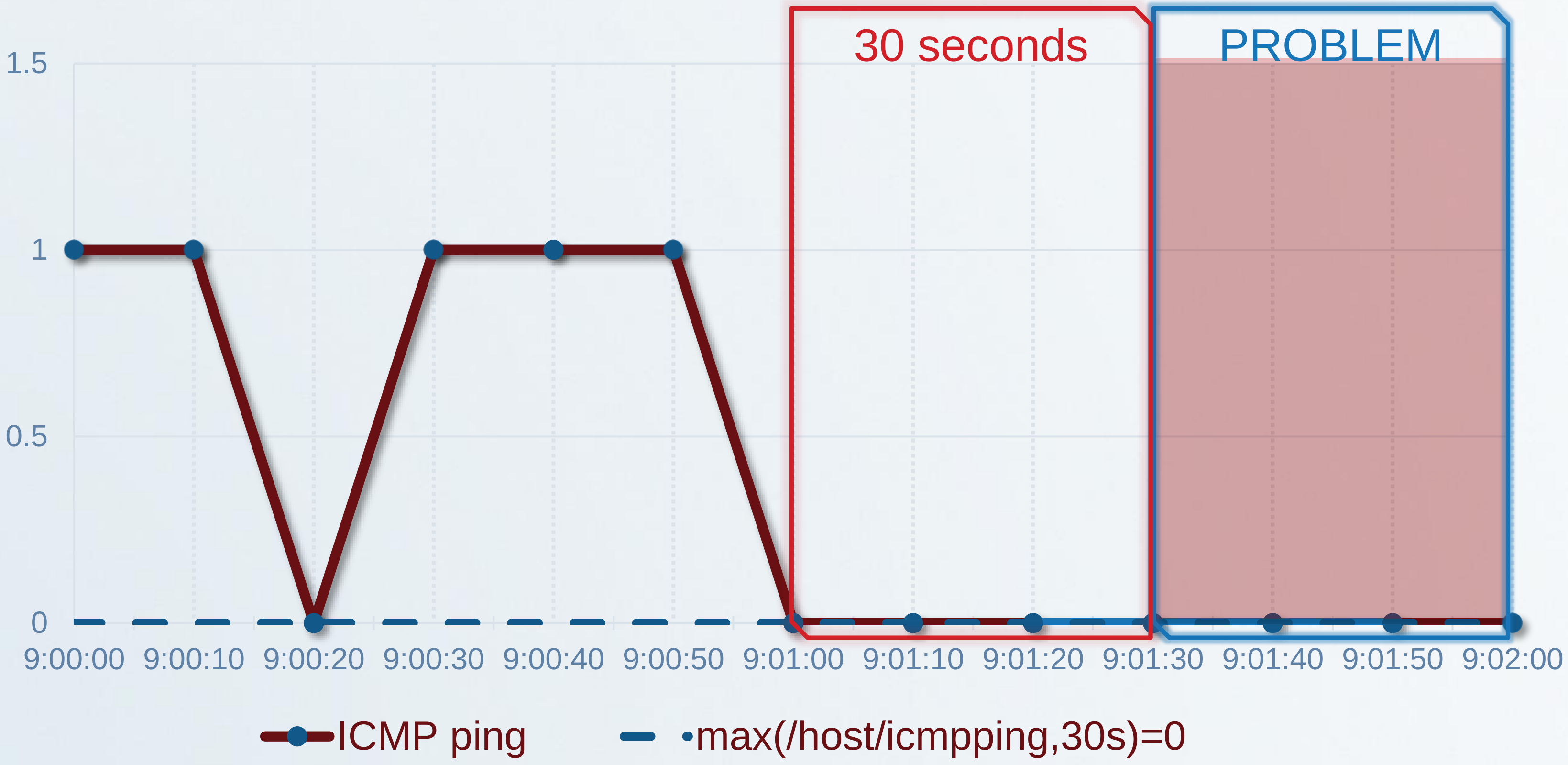
Problem resolves immediately

COMMON MISTAKES AND RECOMMENDATIONS

ZABBIX

The max() function

- Highest value of an item within the defined evaluation period.



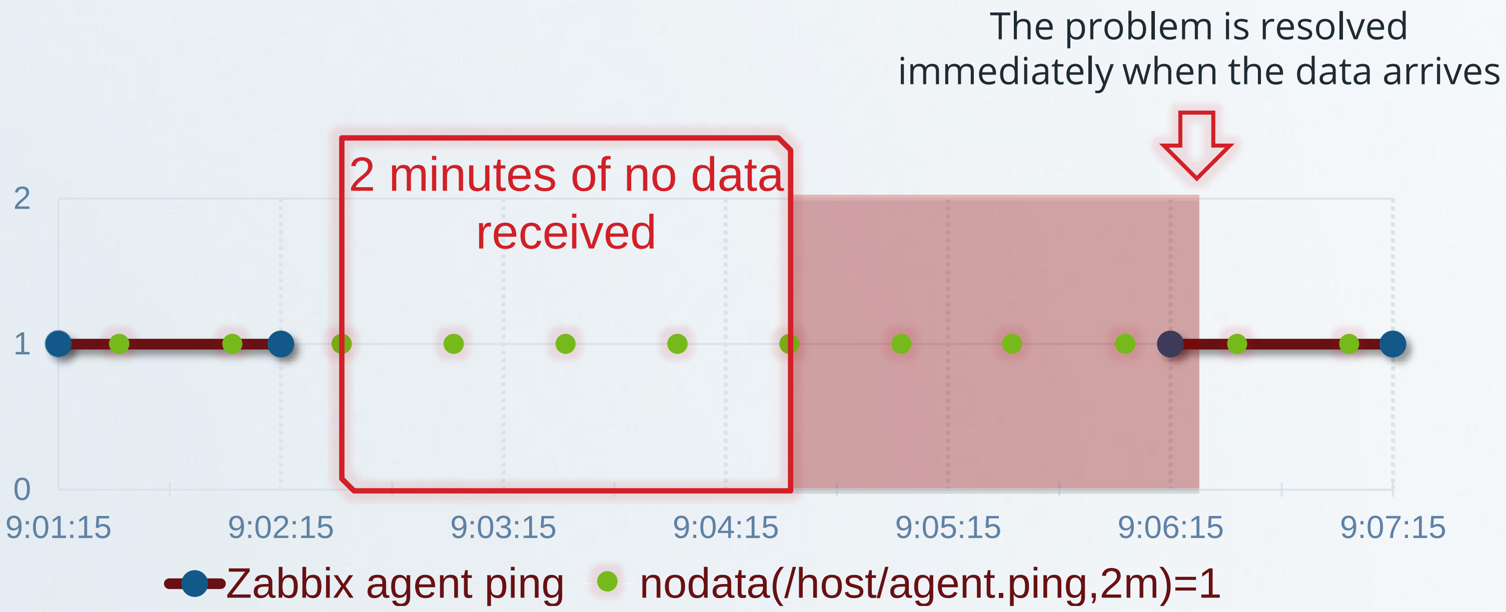
ALERT WHEN THERE IS NO DATA BEING COLLECTED BY AN ITEM

The nodata() function

- ✓ Syntax:

  nodata(/host/key,time period,<mode>)

- ✓ Time can’t be defined as less than 30 seconds
- ✓ Returns 1 – if no data received during the defined period of time
- ✓ Returns 0 – otherwise



The problem is resolved immediately when the data arrives

2 minutes of no data received

ALERT WHEN THERE IS NO DATA BEING COLLECTED BY AN ITEM

ZABBIX

Notes on nodata() function

- nodata() x proxy:
  - ✓ The nodata() triggers monitored by proxies are, by default, sensitive to the proxy availability
  - ✓ They will not fire if the data is expected from a proxy which is currently offline
  - ✓ You can make use of the “strict” mode to ignore the proxy availability
- nodata() can return some false positives if:
  - ✓ There’s time sync issues between Zabbix server, proxy, and agent
  - ✓ The discard unchanged preprocessing steps are used
  - ✓ History is not saved for the item

LONG PERIOD DATA EVALUATION

Let’s talk a little about Cache usage

- Value cache
  - ✓ Value Cache stores values needed for trigger calculations and calculated items
  - ✓ Used to access historical data, instead of making direct SQL calls to the database
  - ✓ Is controlled by the ValueCacheSize (0, 128K-64G) parameter in Zabbix server configuration file
  - ✓ Example:

    Function last(#10) keeps 9 latest values in value cache

    Function avg(1h) keeps 1 hour of data in value cache
- Only if some value is missing in the cache, the history syncer will read it from the Database and insert into the cache.

LONG PERIOD DATA EVALUATION

Sometimes we want to evaluate the behavior of our systems considering months, even years.

- Using the already mentioned functions is not ideal for the job
- There’s a specific set of functions designed for this called Trend functions
  - ✓ trendfunction(period,period_shift)
  - ✓ period - the time period (minimum '1h'), defined as <N><time unit>:

    N - number of time units

    time unit - h (hour), d (day), w (week), M (month) or y (year)
  - ✓ period_shift - the absolute time period

LONG PERIOD DATA EVALUATION

Some examples for Trend Functions:

trendavg(/host/key,1h:now/h) - #the average for the previous hour (e.g. 12:00-13:00)

trendcount(/host/key,1h:now/h-1h) - #the value count for two hours ago (11:00-12:00)

trendsum(/host/key,1h:now/h-2h) - #the sum for three hours ago (10:00-11:00)

trendmax(/host/key,1M:now/M-1y) - #the maximum for the previous month a year ago

trendmin(/host/key,1M:now/M-1y) - #the minimum for the previous month a year ago

LONG PERIOD DATA EVALUATION

ZABBIX

Notes on the Trend Function Cache

- In contrast to history functions, they use trend data for calculation
- Trends store hourly aggregate values. Trend functions use these hourly averages, and thus are useful for long-term analysis
- Trend function results are cached so multiple calls to the same function with the same parameters fetch info from the database only once.
- The trend function cache is controlled by the TrendFunctionCacheSize (128K-2G) server parameter.

ZABBIX

THANK YOU!

Victor Credidio

Support Engineer and Certified Trainer