ZABBIX 6.0 WORKSHOP WEEK

CREATING TRIGGERS FOR BASELINE MONITORING AND ANOMALY DETECTION

01

ZABBIX
6.0

ANOMALLY DETECTION

WHAT IS ANOMALLY DETECTION

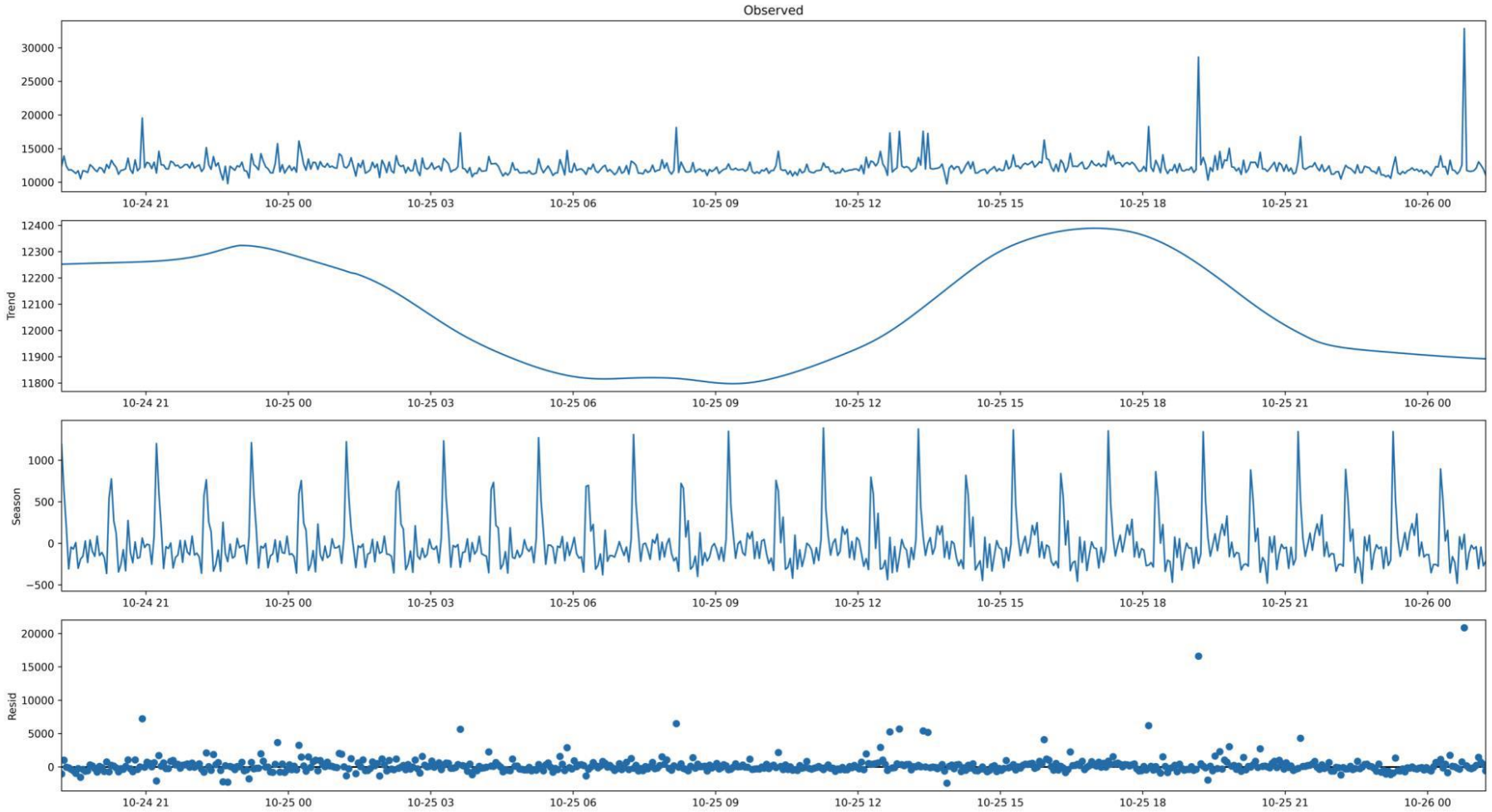
ZABBIX 6.0

- Anomally detection works by going through historical data and looking for values that are out of normal
- Works if the majority of data is considered «normal»
- Long term analitics – works with trends data
- Zabbix uses STL decomposition algorithm (Seasonal and Trend decomposition using Loess)

WHAT IS STL DECOMPOSITION ALGORITHM?

ZABBIX 6.0

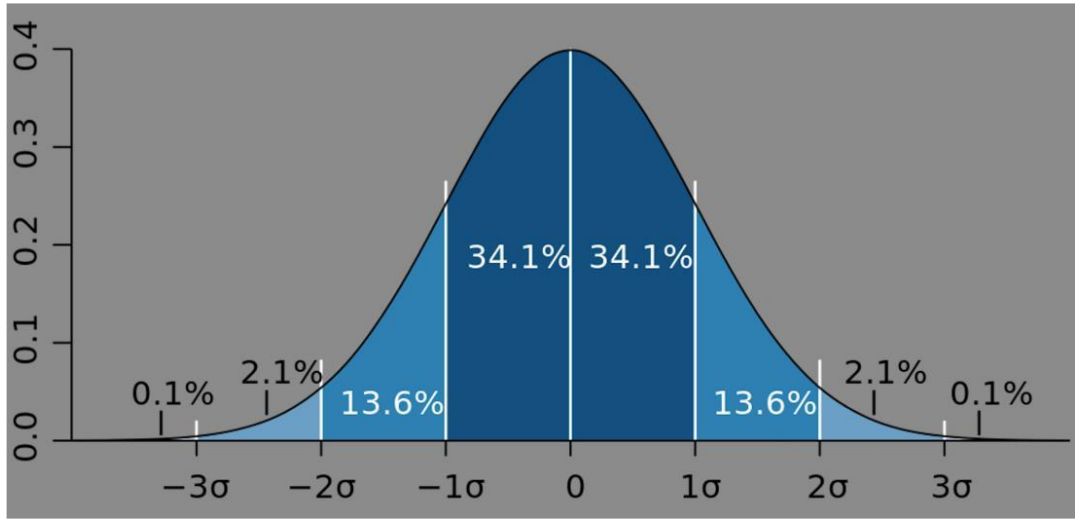
Decomposition using STL algorithm is a way to split a single time series sequence into three other sequences:



DEVIATIONS

Deviation is a measure of data variability.

How “far” values are from average?

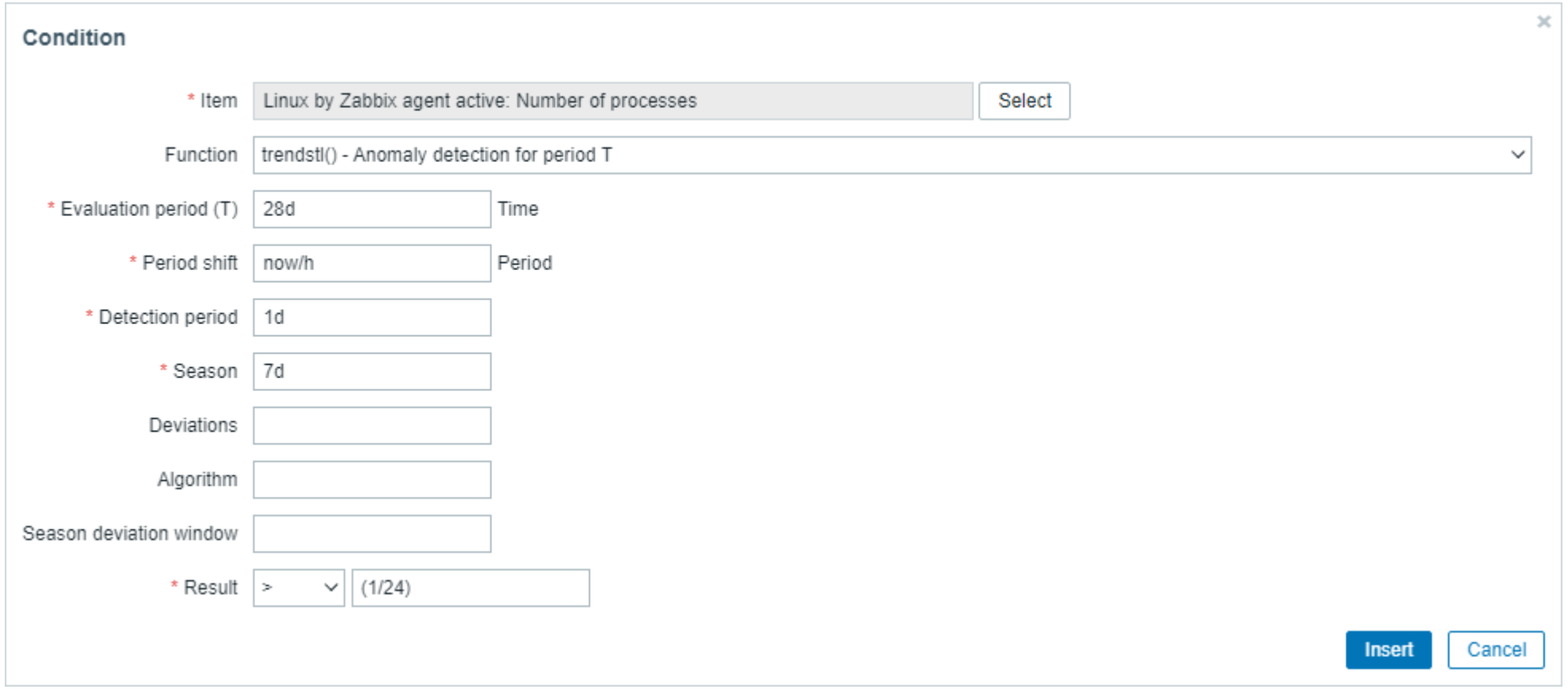


Zabbix has capabilities to determine deviation in multiple ways.

FIND ANOMALY RATE WITH TRENDSTL

ZABBIX 6.0

Data to work with: 28d, start to analyze starting from previous hour, use ‘1d’ to seek anomalies, weekdays matters (Season: 7d). Deviations – how many is considered as anomally (default: 3)



OUTPUT OF TRENDSTL FUNCTION

ZABBIX 6.0

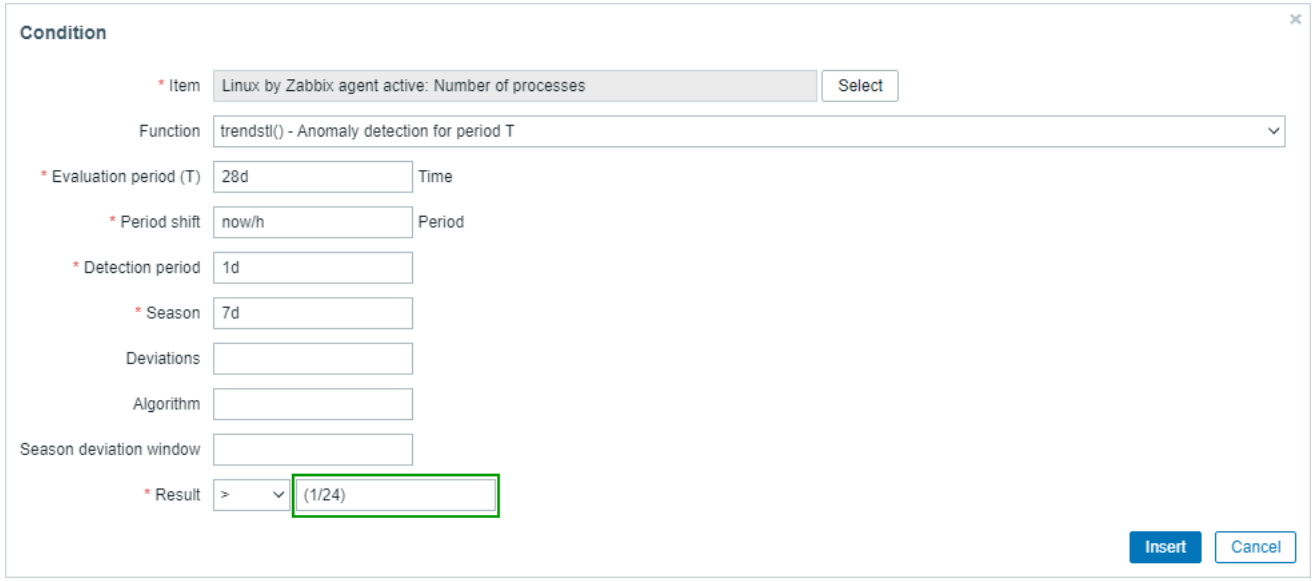
- a decimal value between 0 and 1
- (the number of anomaly values in detect period) / (total number of values in detect period).

Example 1: Context is 7d, detect anomalies in last 1d. If one is detected, then reported value is:

1/24 = 1 anomally detected within last 24h

Example 2: Context is 7d, detect anomalies for last 2d. If one is detected, then reported value is:

1/48 = 1 anomally detected within last 48h



DEVIATION ALGORITHMS

- mad (default) – «median absolute deviation»

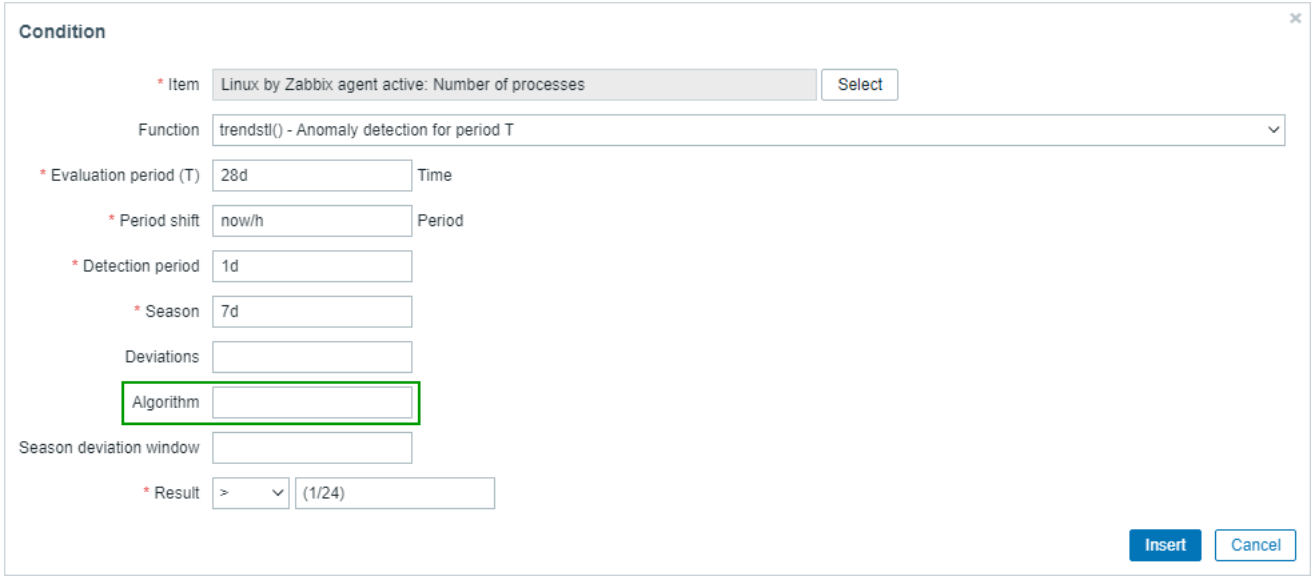
  A robust measure of the variability of a univariate sample of quantitative data.

- stddevpop – «population standard deviation»

  Looks at the square root of the variance of the set of numbers.

- stddevsamp – «sample standard deviation»

  Average distance of the observed data from the expected values

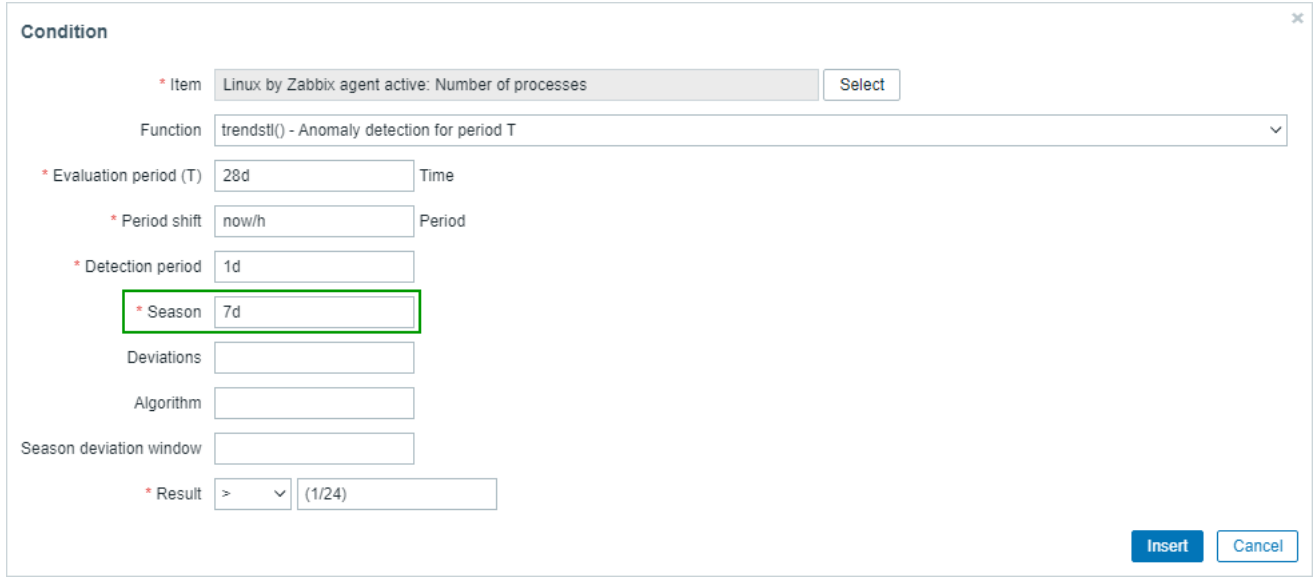


CONCEPT OF SEASION DATA

ZABBIX 6.0

How the service has been used:

- All days are the same (24h scale)
- All Thuesdays are the same (7d scale)
- 8h working day in a 24/7 factory. There are 3 sessions in the level of 1d.
- First day of each month



CONCLUDION

ZABBIX 6.0

- Get trend values from the period
- Decompose values, get reminder
- Calculate deviation for values in remainder
- Select values with deviation and compare with threshold

02

ZABBIX
6.0

BASELINE MONITORING

WHAT IS BASELINE MONITORING?

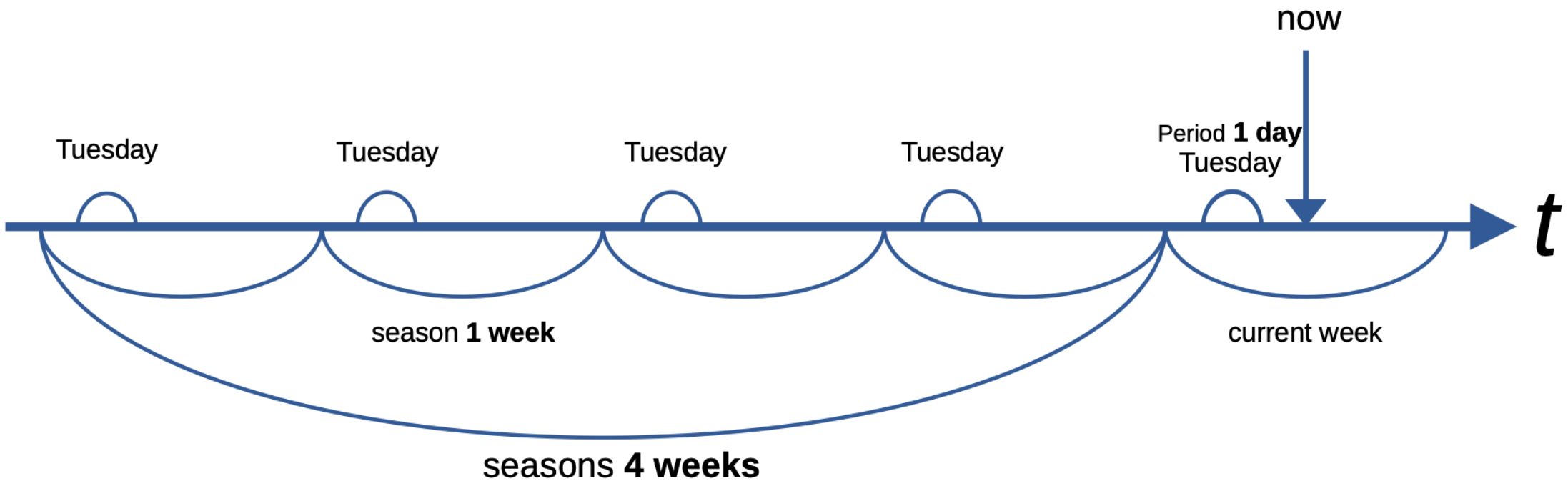
- Baseline is a value derived from an average over multiple calendar periods of the same length.

BASELINE PROPERTIES

ZABBIX 6.0

- Periods and seasons.
- Average from past calendar period:
  - E.g., every Monday of the past 4 weeks
  - Monday is a period, week is a season
- Periods are linked to current time:
  - If today is Wednesday, then periods are Tuesdays

PERIODS VS SEASONS



2 WAYS TO CALCULATE BASELINE

ZABBIX 6.0

- ‘baselinewma’ - Calculates the baseline by averaging data from the same timeframe in multiple equal time periods ('seasons') using the weighted moving average (WMA) algorithm.

- ‘baselinedev’ - Returns the number of deviations (by stddevpop algorithm) between the last data period and the same data periods in preceding seasons.

BASELINE WEIGHTED MOVING AVERAGE

ZABBIX 6.0

Check if CPU usage is 2x higher than WMA on the same weekdays over last 5 days (exclusive)

Triggers	Key	Interval	History	Trends	Type	Status
Triggers 2	system.cpu.util		7d	365d	Dependent item	Enabled

Severity	Name	Expression	Status
Warning	High CPU utilization (over {$CPU.UTIL.CRIT}% for 5m)	**min(**/Linux by Zabbix agent active/system.cpu.util,5m**)**>{$CPU.UTIL.CRIT}	Enabled
Average	CPU usage 2x bigger than in the last 5 seasons(d) (same last 4h)	**baselinewma(**/Linux by Zabbix agent active/system.cpu.util,4h:now/h,"d",5**)***2 < **trendavg(**/Linux by Zabbix agent active/system.cpu.util,4h:now/h**)**	Enabled

COUNT OF DEVIATIONS

ZABBIX 6.0

More than 3 deviations detected in the last 8h, by using using input periods from 12 weeks.

Triggers	Key	Interval	History	Trends	Type	Status
Triggers 1	system.cpu.switches	1m	7d	365d	Zabbix agent (active)	Enabled

Severity	Name	Expression	Status
Average	More than 3 deviations detected in the last 8h by using weekly input from last 12w	**baselinedev(**/Linux by Zabbix agent active/system.cpu.switches,8h:now/h,"w",12)>3	Enabled

ZABBIX

6.0

Thank you

www.zabbix.com