

ZABBIX

6.0

WORKSHOP  
WEEK

CREATING TRIGGERS  
FOR BASELINE MONITORING  
AND ANOMALY DETECTION



# 01

## ANOMALLY DETECTION

ZABBIX

6.0



# WHAT IS ANOMALLY DETECTION

- ✓ Anomaly 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 analytics – works with trends data
- ✓ Zabbix uses STL decomposition algorithm (Seasonal and Trend decomposition using Loess)

# WHAT IS **STL** DECOMPOSITION ALGORITHM?

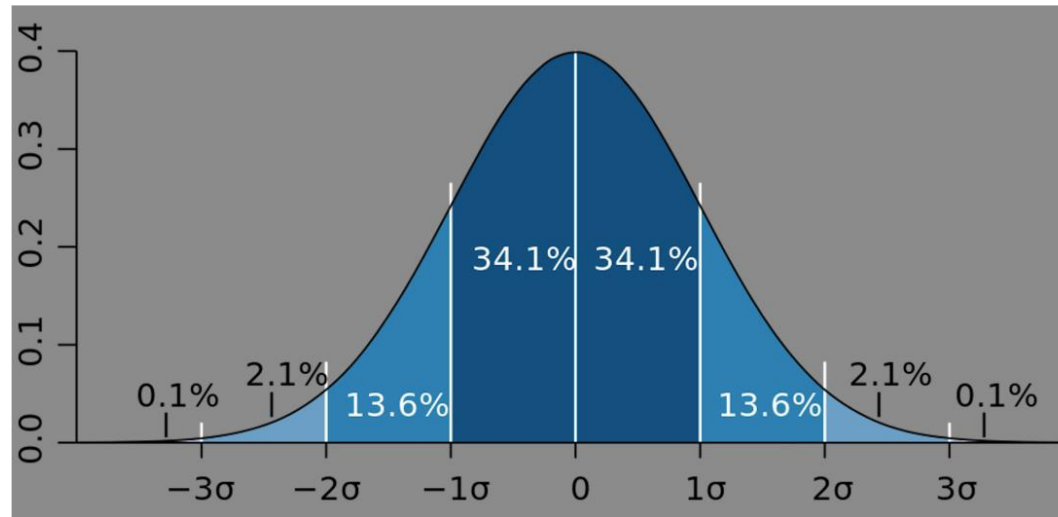
Decomposition using **STL algorithm** is a way to split a single time series sequence into three other sequences:



# 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

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 anomaly (default: 3)

**Condition** ✕

\* Item

Function

\* Evaluation period (T)  Time

\* Period shift  Period

\* Detection period

\* Season

Deviations

Algorithm

Season deviation window

\* Result

# OUTPUT OF TRENDSTL FUNCTION

- ✓ 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:

$1/24 = 1$  anomaly detected within last 24h

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

$1/48 = 1$  anomaly detected within last 48h

The screenshot shows the 'Condition' configuration window in Zabbix. The 'Item' is set to 'Linux by Zabbix agent active: Number of processes'. The 'Function' is 'trendstl() - Anomaly detection for period T'. The 'Evaluation period (T)' is '28d'. The 'Period shift' is 'now/h'. The 'Detection period' is '1d'. The 'Season' is '7d'. The 'Result' is '>' with a value of '(1/24)' entered in the adjacent field. The 'Insert' and 'Cancel' buttons are visible at the bottom right.

* Item	Linux by Zabbix agent active: Number of processes	Select
Function	trendstl() - Anomaly detection for period T	
* Evaluation period (T)	28d	Time
* Period shift	now/h	Period
* Detection period	1d	
* Season	7d	
Deviations		
Algorithm		
Season deviation window		
* Result	>	(1/24)

# 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

The screenshot shows the 'Condition' configuration window in Zabbix. The 'Item' field is set to 'Linux by Zabbix agent active: Number of processes'. The 'Function' is 'trendstl() - Anomaly detection for period T'. The 'Evaluation period (T)' is '28d', 'Period shift' is 'now/h', 'Detection period' is '1d', and 'Season' is '7d'. The 'Algorithm' field is currently empty and highlighted with a green border. The 'Result' is set to '>' and '(1/24)'. The 'Insert' and 'Cancel' buttons are at the bottom right.



# CONCEPT OF SEASON DATA

How the service has been used:

- ✓ All days are the same (24h scale)
- ✓ All Tuesdays 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

The screenshot shows the 'Condition' configuration window in Zabbix. The 'Season' field is highlighted with a green box and contains the value '7d'. Other fields include 'Item' (Linux by Zabbix agent active: Number of processes), 'Function' (trendstl() - Anomaly detection for period T), 'Evaluation period (T)' (28d), 'Period shift' (now/h), 'Detection period' (1d), 'Deviations', 'Algorithm', 'Season deviation window', and 'Result' (> (1/24)).

* Item	Linux by Zabbix agent active: Number of processes	Select
Function	trendstl() - Anomaly detection for period T	
* Evaluation period (T)	28d	Time
* Period shift	now/h	Period
* Detection period	1d	
* Season	7d	
Deviations		
Algorithm		
Season deviation window		
* Result	>	(1/24)

# CONCLUSION

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

# 02

ZABBIX

6.0

## BASELINE MONITORING



# WHAT IS BASELINE MONITORING?

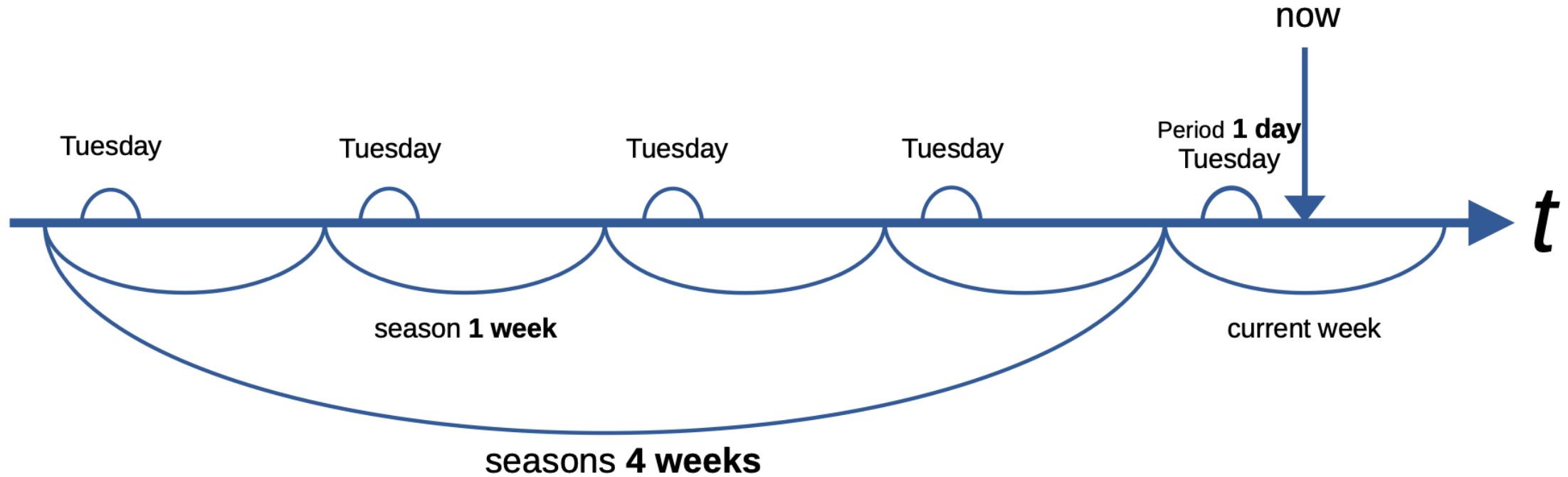
- Baseline is a value derived from an average over multiple calendar periods of the same length.



# BASELINE PROPERTIES

- ✓ 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

- ④ 'baseline`wma`' - Calculates the baseline by averaging data from the same timeframe in multiple equal time periods ('seasons') using the `weighted moving average` (WMA) algorithm.
- ④ 'baseline`dev`' - 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

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)	<code>min(/Linux by Zabbix agent active/system.cpu.util,5m)&gt;{CPU.UTIL.CRIT}</code>	Enabled
Average	CPU usage 2x bigger than in the last 5 seasons(d) (same last 4h)	<code>baselinewma(/Linux by Zabbix agent active/system.cpu.util,4h:now/h,"d",5)*2 &lt; trendavg(/Linux by Zabbix agent active/system.cpu.util,4h:now/h)</code>	Enabled



# COUNT OF DEVIATIONS

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

Triggers	Key	Interval	History	Trends	Type	Status
<a href="#">Triggers 1</a>	system.cpu.switches	1m	7d	365d	Zabbix agent (active)	<a href="#">Enabled</a>

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

ZABBIX

6.0

Thank you

[www.zabbix.com](http://www.zabbix.com)

