ZABBIX SUMMIT

OCTOBER 8 · 10, 2025
RIGA · LATVIA

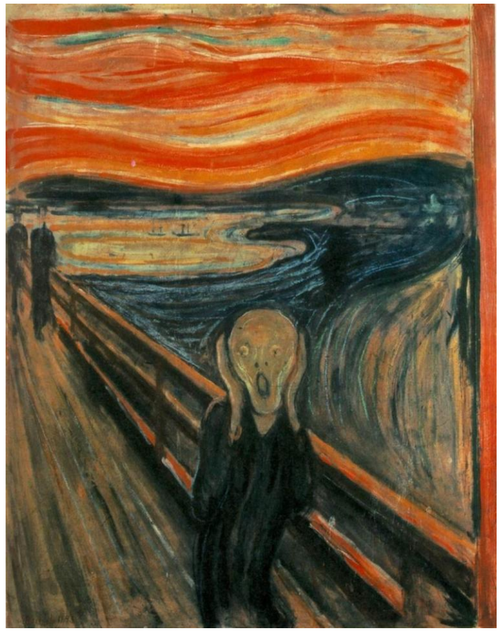
Trigger Mastery in Zabbix

Practical Tips and Deep Insights

ZABBIX SUMMIT
OCTOBER 8 · 10, 2025
RIGA · LATVIA

The problem(s)

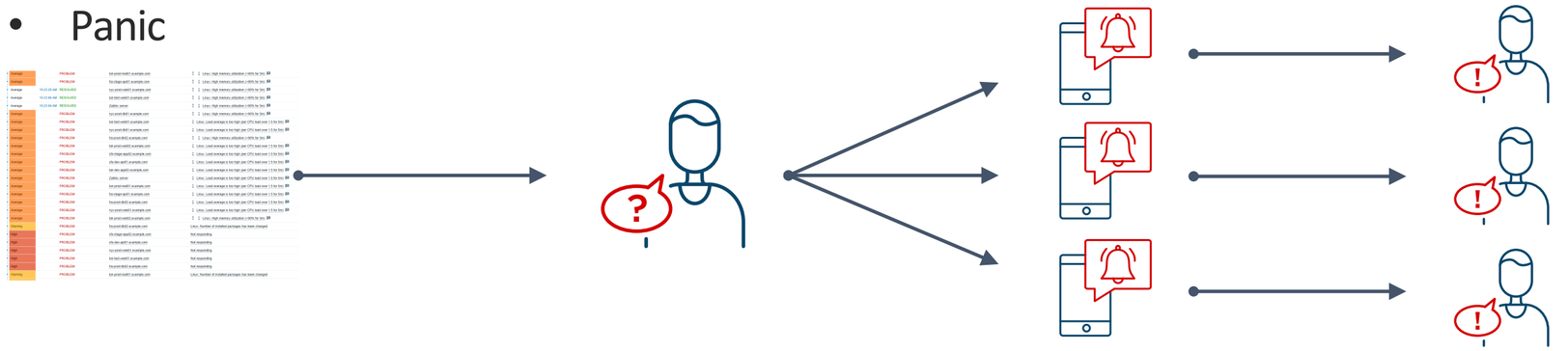
Average		PROBLEM	lon-prod-mail01.example.com	Linux: High memory utilization (>90% for 5m)
Average		PROBLEM	fra-stage-api01.example.com	Linux: High memory utilization (>90% for 5m)
Average	10:23:20 AM	RESOLVED	nyc-prod-web01.example.com	Linux: High memory utilization (>90% for 5m)
Average	10:23:06 AM	RESOLVED	lon-test-web01.example.com	Linux: High memory utilization (>90% for 5m)
Average	10:23:04 AM	RESOLVED	Zabbix server	Linux: High memory utilization (>90% for 5m)
Average		PROBLEM	nyc-prod-db01.example.com	Linux: High memory utilization (>90% for 5m)
Average		PROBLEM	lon-test-web01.example.com	Linux: Load average is too high (per CPU load over 1.5 for 5m)
Average		PROBLEM	nyc-prod-db01.example.com	Linux: Load average is too high (per CPU load over 1.5 for 5m)
Average		PROBLEM	fra-prod-db02.example.com	Linux: High memory utilization (>90% for 5m)
Average		PROBLEM	tok-prod-web02.example.com	Linux: Load average is too high (per CPU load over 1.5 for 5m)
Average		PROBLEM	sfo-stage-app02.example.com	Linux: Load average is too high (per CPU load over 1.5 for 5m)
Average		PROBLEM	sfo-dev-api01.example.com	Linux: Load average is too high (per CPU load over 1.5 for 5m)
Average		PROBLEM	tok-dev-app03.example.com	Linux: Load average is too high (per CPU load over 1.5 for 5m)
Average		PROBLEM	Zabbix server	Linux: Load average is too high (per CPU load over 1.5 for 5m)
Average		PROBLEM	lon-prod-mail01.example.com	Linux: Load average is too high (per CPU load over 1.5 for 5m)
Average		PROBLEM	fra-stage-api01.example.com	Linux: Load average is too high (per CPU load over 1.5 for 5m)
Average		PROBLEM	fra-prod-db02.example.com	Linux: Load average is too high (per CPU load over 1.5 for 5m)
Average		PROBLEM	nyc-prod-web01.example.com	Linux: Load average is too high (per CPU load over 1.5 for 5m)
Average		PROBLEM	tok-prod-web02.example.com	Linux: High memory utilization (>90% for 5m)
Warning		PROBLEM	fra-prod-db02.example.com	Linux: Number of installed packages has been changed
High		PROBLEM	sfo-stage-app02.example.com	Not responding
High		PROBLEM	sfo-dev-api01.example.com	Not responding
High		PROBLEM	nyc-prod-web01.example.com	Not responding
High		PROBLEM	lon-test-web01.example.com	Not responding
High		PROBLEM	fra-prod-db02.example.com	Not responding
Warning		PROBLEM	lon-prod-mail01.example.com	Linux: Number of installed packages has been changed



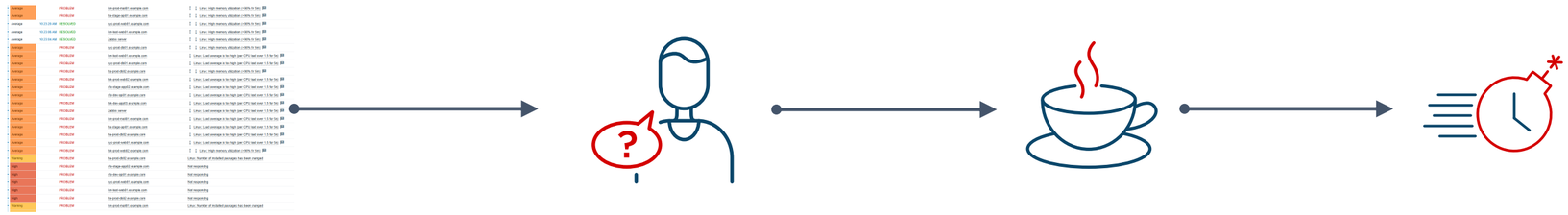
Too many problems

Cause two types of reactions

- Panic



- Nerve



ZABBIX SUMMIT
OCTOBER 8 · 10, 2025
RIGA · LATVIA

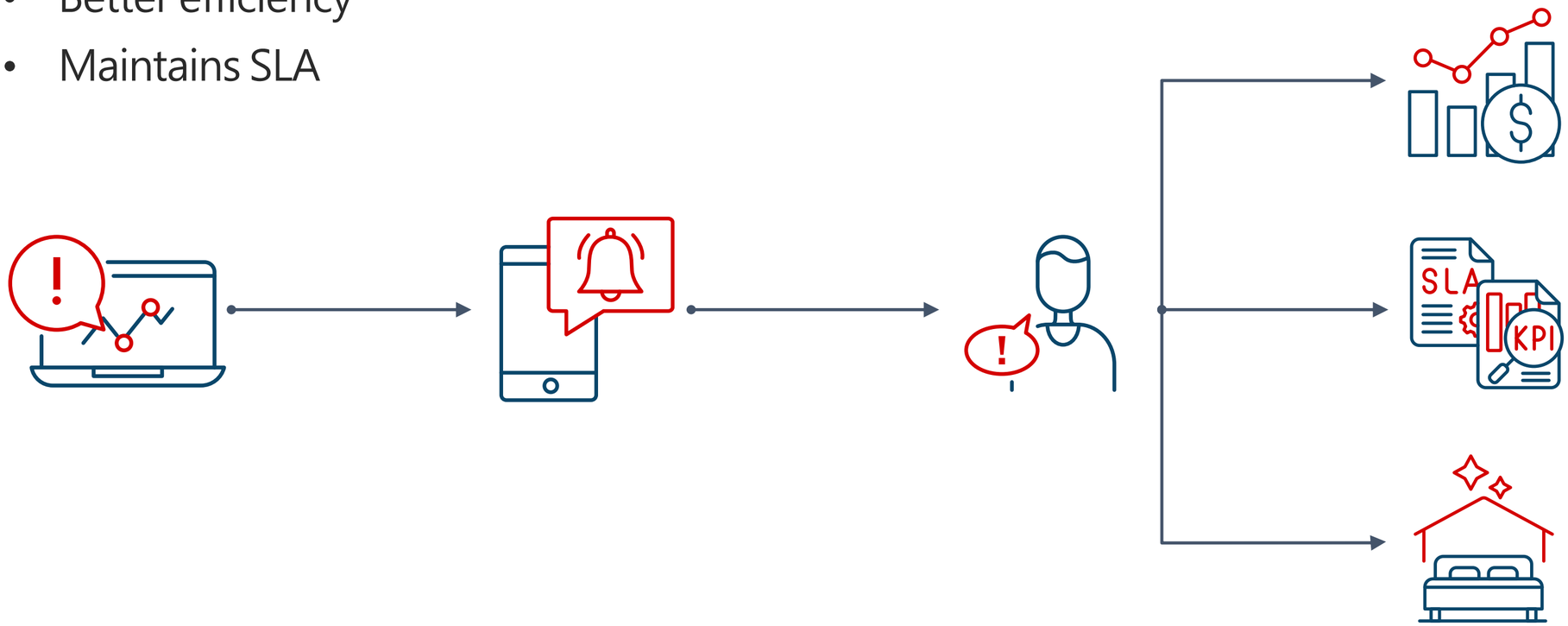
The solution

Updating trigger goals

Proper trigger configuration

Reduce MTTR

- Continuous improvement
- Better efficiency
- Maintains SLA

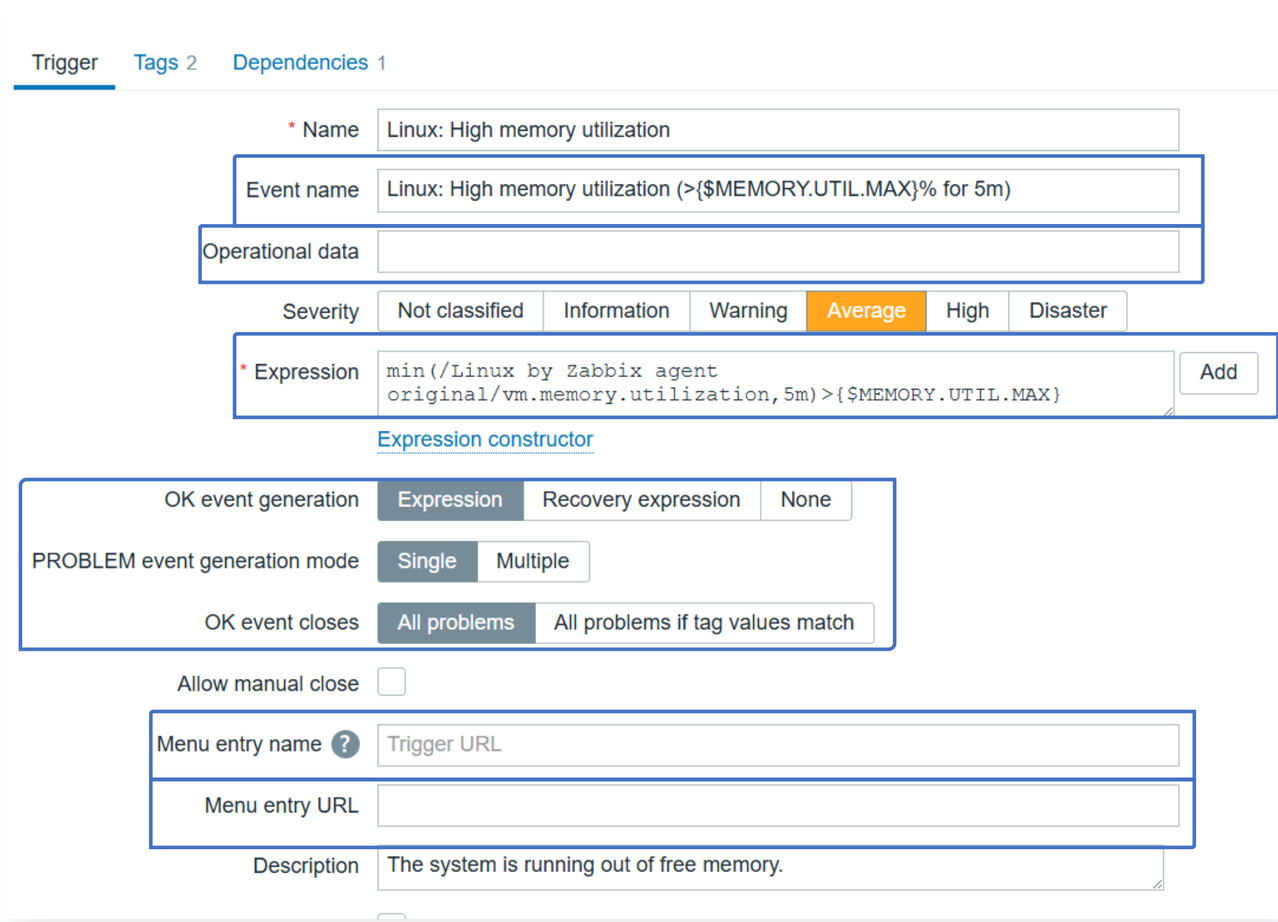


Common triggers - common problems

ZABBIX SUMMIT
OCTOBER 8 · 10, 2025
RIGA · LATVIA

Improving trigger:

- Event name
- Op. data
- Expressions
- OK events
- Menu entry
- Description
- Tags



Event name

ZABBIX SUMMIT

OCTOBER 8 · 10, 2025
RIGA · LATVIA

Event name supports the following macros:

- Regular problem names:
  - Load average is too high
  - Linux: Number of installed packages has been changed
  - SSL certificate is expiring
  - ORA error in the log
  - snmptrap notification error
  - Power state alarm

- All of those are real trigger names
- All of those raise many questions
- All of them can be better!

Event name supports the following macros:

- Expression macro
  - {?TRIGGER(/LIKE/EXPRESSION)}
- User macro
  - {$CUSTOM.USER.MACRO}
- Date/time macros
  - {TIME}, {TIMESTAMP}
- Host and item macros
  - {HOST.CONN}, {HOST.DNS}, {ITEM.LASTVALUE*}, {ITEM.LOG.*}, etc
- Function and trigger macros
  - {FUNCTION.VALUE}, {FUNCTION.RECOVERY.VALUE}, {TRIGGER.EXPRESSION.EXPLAIN}
- Macro functions
  - fmtnum(), fmttime(), regsub()

Improving problem names using user and expression macros:

- Expression macro
  - {?TRIGGER(/LIKE/EXPRESSION)}
  - {?avg(/Linux server/proc.num,10m)}

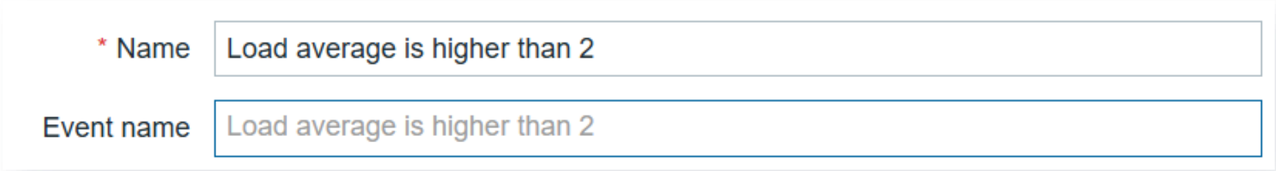
Function

Hostname or template name

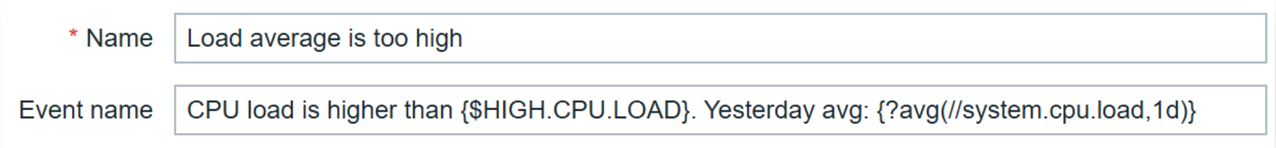
Item key

Function parameters

- Before
  - CPU load is higher than 2



- After
  - CPU load is higher than 2. Yesterday avg: 0.14200555170020829
  - CPU load is higher than 2. Last week avg: 0.11020166431792559



Too precise? Format the number

- The fmtnum() function reduces the number of digits using rounding
- {{MACRO}.fmtnum(digits)}

Expression macro | **Expression macro** | **Digits after the floating point**

- Before
  - CPU load is higher than 2. Yesterday avg: 0.1450055517002 0829
  - CPU load is higher than 2. Last week avg: 0.1122016643179 2559

* Name	Load average is too high
Event name	CPU load is higher than {$HIGH.CPU.LOAD}. Yesterday avg: {?avg(//system.cpu.load,1d)}

- After
  - CPU load is higher than 2. Yesterday avg: 0.15
  - CPU load is higher than 2. Last week avg: 0.11

* Name	Load average is too high
Event name	CPU load is higher than {$HIGH.CPU.LOAD}. Yesterday avg: {{?avg(//system.cpu.load,1d)}.fmtnum(2)}

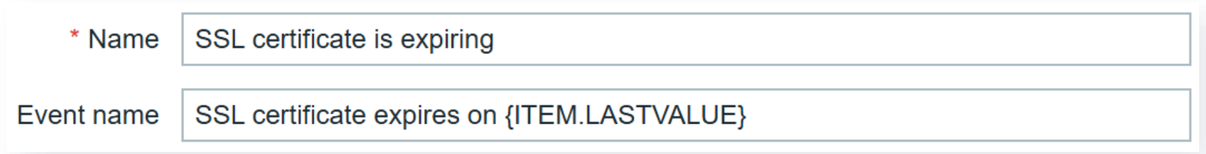
Problem is date-related

Problem is date-related

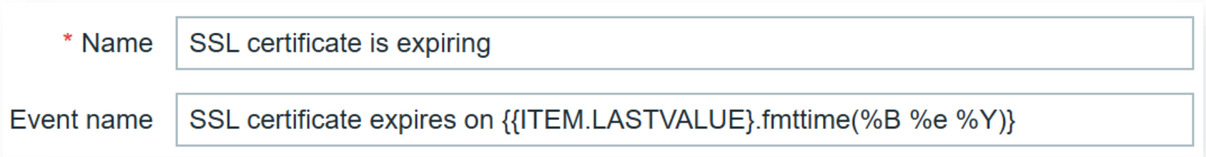
- The fmttime() function allows us to format time
- {{MACRO}.fmttime(format,<time_shift>)}

Expression/ User/Built-in macros	Function	strftime based format	Time shift applied before formatting

- Before
  - Certificate expires on 2025.10.11 12:15:21



- After
  - Certificate expires on October 11 2025

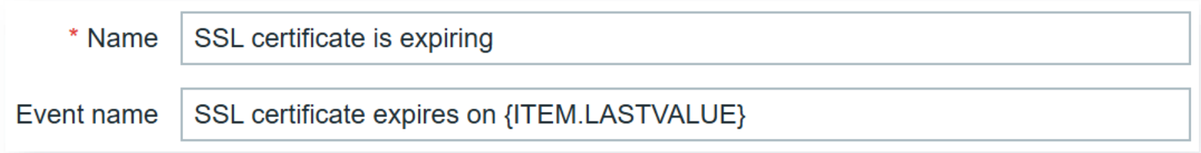


Problem is date-related

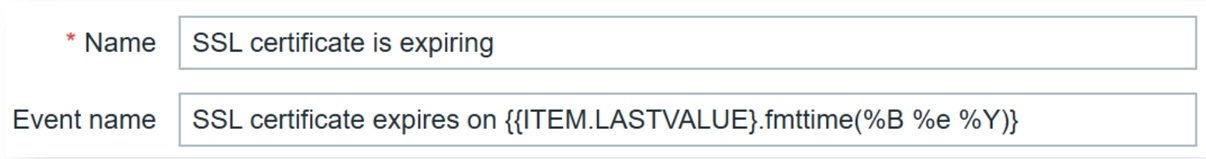
Need to convert the numerical value?

- Need to be even more precise?

- Before
  - Certificate expires on October 11 2025



- After
  - Certificate expires on October 11 2025, in less than 7 days



Problem is text-based (log or snmptraps)

Problem is text-based (log or snmptraps)

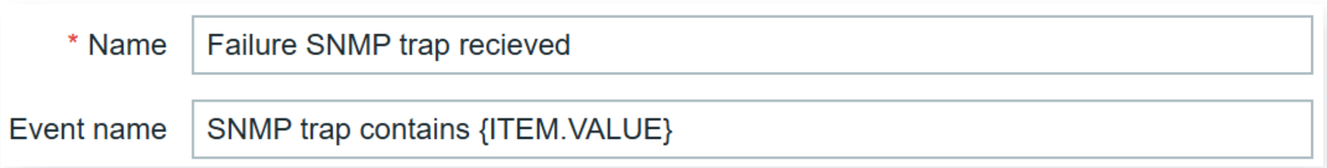
- The regsub() function allows to extract using regexp
- {{MACRO}.regsub(pattern, output)

Output can be customized

- By adding any custom text
- By exctracting problematic value information
  - \1 - \9 returns capture groups.
  - \0 returns the matched text

Problem is text based (log or snmptraps)

- Before
  - SNMP trap contains 15:40:29 2025/09/17 <UNKNOWN>UDP: [127.0.0.1]:60789->[127.0.0.2]:162.1.3.6.1.2.1.1.3.0 32:22:46:17.52.1.3.6.1.6.3.1.1.4.1.0 .1.3.6.1.4.1.164.15.0.164050.1.3.6.1.4.1.164.15.1.3.0 127.0.0.2.1.3.6.1.4.1.164.15.1.4.0 /AGGREGATOR.1.3.6.1.4.1.164.15.1.5.0 APE2000.1.3.6.1.4.1.164.15.1.6.0 PW 26.1.3.6.1.4.1.164.15.1.2.0 abnormal.1.3.6.1.4.1.164.15.1.7.0 PW Down (DEV-01 (DEV-01/MICRO), Peer: 127.0.0.1 (DEV-01/MICRO)).1.3.6.1.4.1.164.15.1.8.0 failure.1.3.6.1.4.1.164.15.1.9.0 noOperation.1.3.6.1.4.1.164.15.1.10.0 425.1.3.6.1.4.1.164.15.1.11.0 EXAMPLE.1.3.6.1.4.1.164.15.1.12.0 NA.1.3.6.1.4.1.164.6.2.11.1.4.1 0.1.3.6.1.4.1.164.15.1.13 2020-12-17 15:52:47.1.3.6.1.6.3.1.1.4.3.0 .1.3.6.1.4.1.164.15.1.3.6.1.6.3.18.1.3.0 192.168.79.220.1.3.6.1.6.3.18.1.4.0 "public"



- After
  - SNMP trap contains Down (DEV-01 (DEV-01/MICRO), Peer: 127.0.0.1 (DEV-01/MICRO))

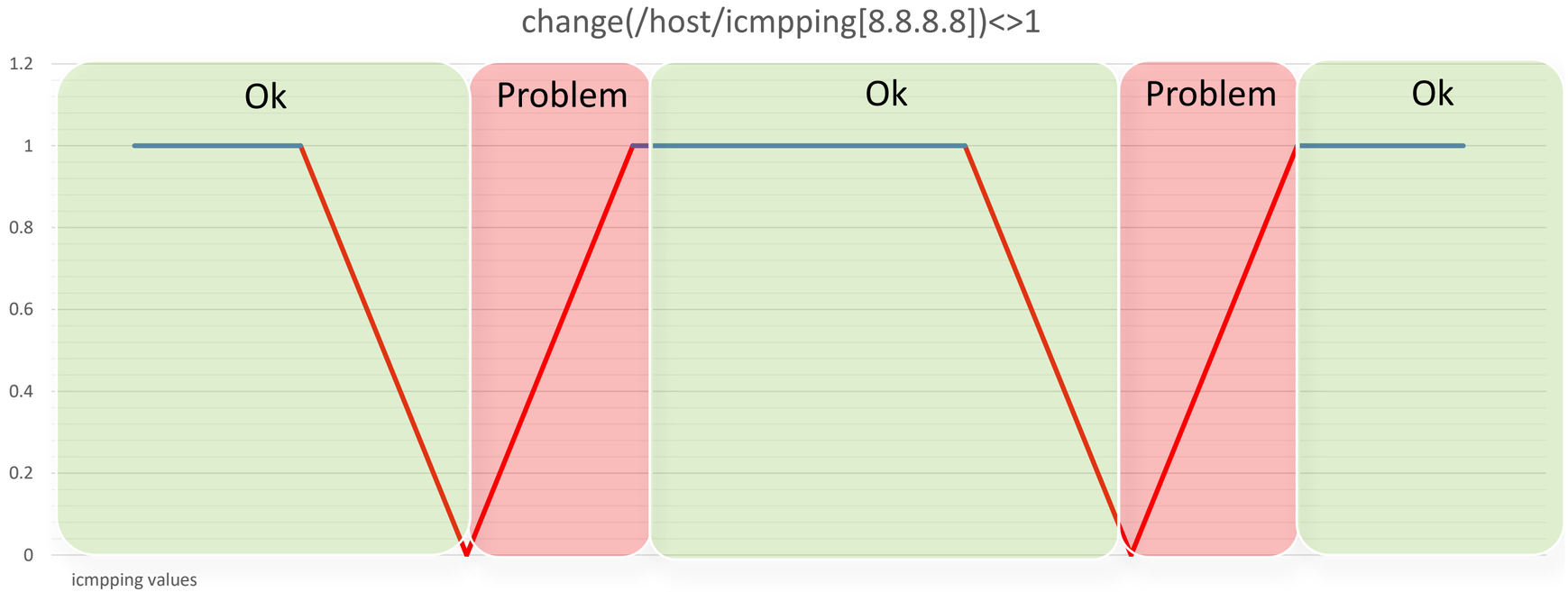
ZABBIX SUMMIT

OCTOBER 8 · 10, 2025
RIGA · LATVIA

Trigger expressions

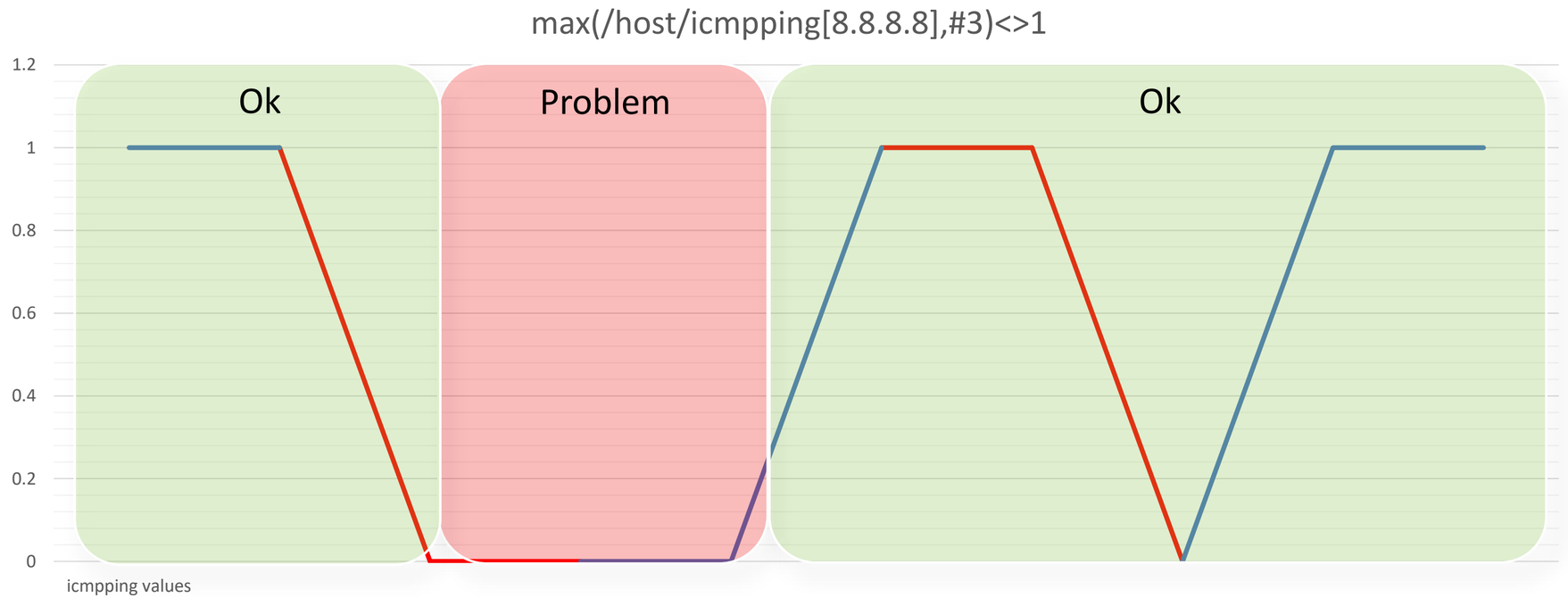
Most common misstep

- Using sensitive functions for fluctuating data:
  - last(/host/net.if.in[eth0])>100M
  - change(/host/icmpping[8.8.8.8])<>1
  - nodata(/host/log[/var/log/messages,error],30)=0



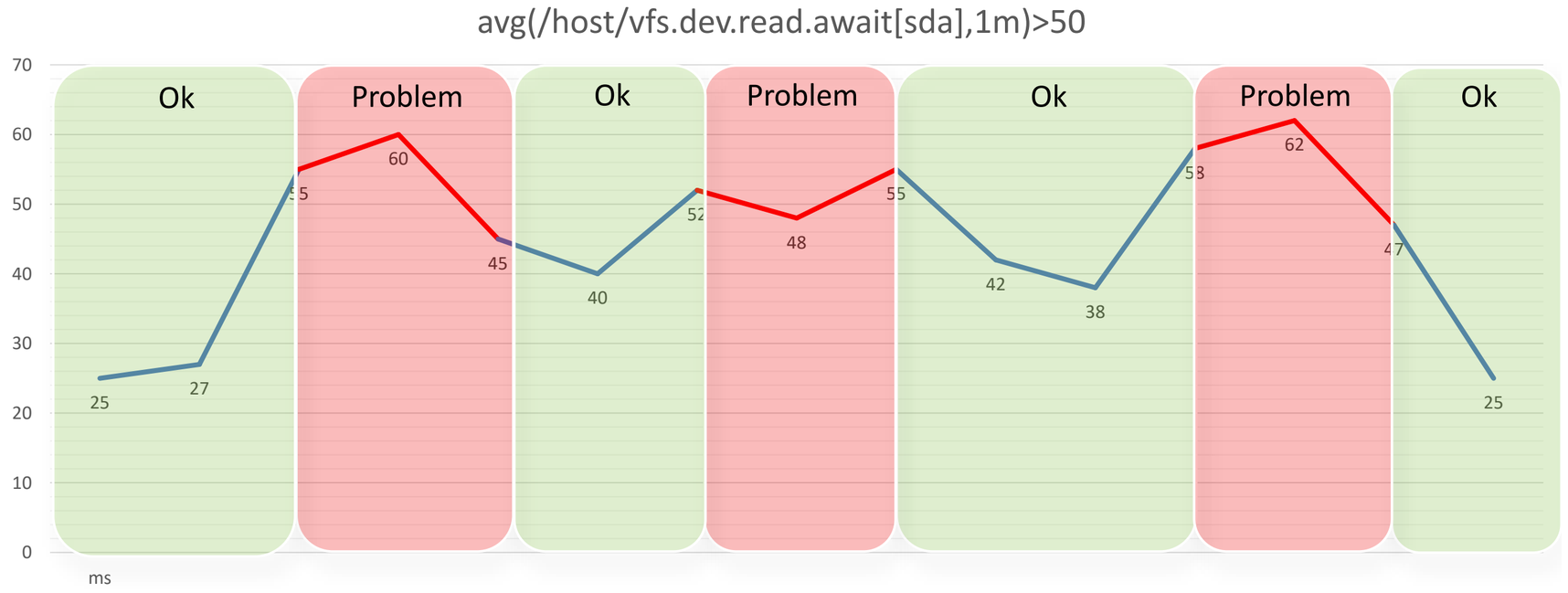
Solution - evaluate data

- Use better functions for evaluating fluctuating data:
  - avg(/host/net.if.in[eth0],5m)>100M
  - max(/host/icmpping[8.8.8.8],#3)=0
  - find(/host/log[/var/log/messages,error],10m,"like","error")=1



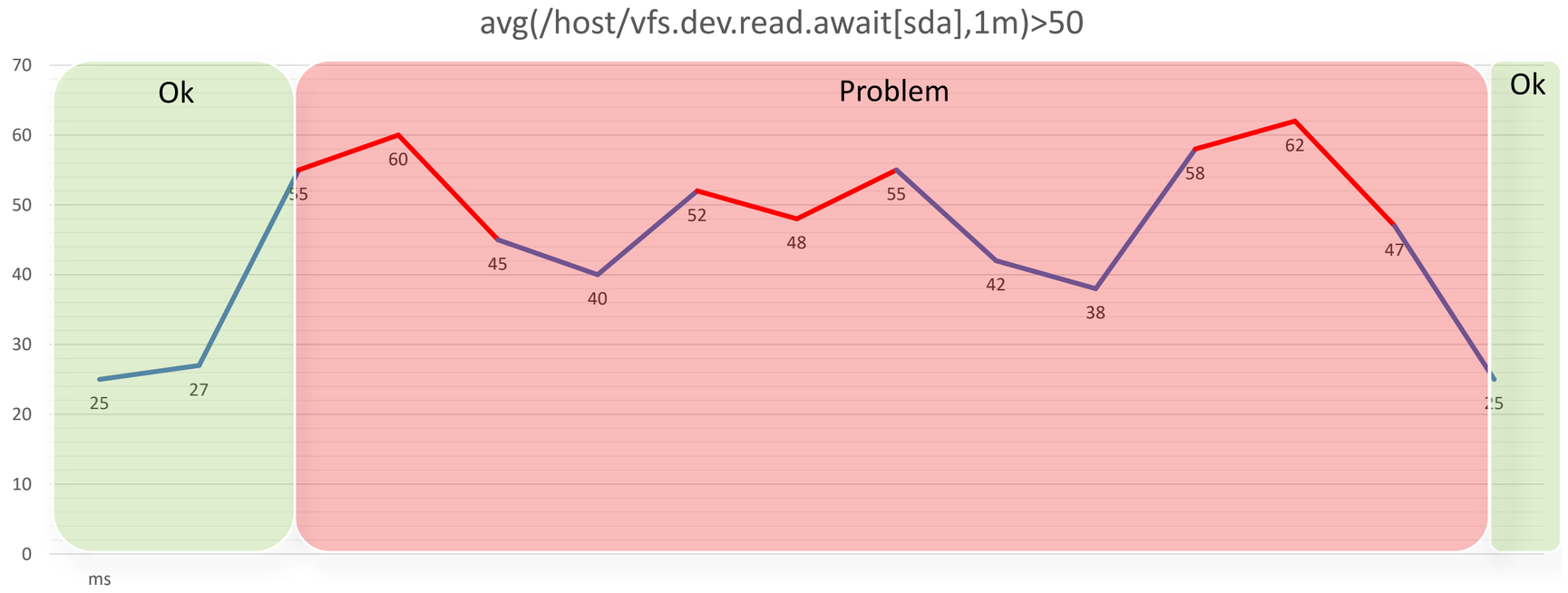
Misstep - using only problem expression

- Relying on problem condition only - may cause trigger flapping
  - last(/host/vfs.fs.size[/,pfree])<20
  - avg(/host/vfs.dev.read.await[sda],1m)>50



Fix - using recovery expression

- Recovery expression will make problem resolution more precise
  - Problem expression:
    avg(/host/vfs.dev.read.await[sda],1m)>50
  - Recovery expression:
    {server:vfs.dev.read.await[sda].avg(5m)}<30



Log/snmptrap missteps

Creating a single trigger for any error:

- find(/host/log[/var/log/messages,"error"],10m,"like","error")=1
- count(/host/snmptrap["failed"],#5)>3

The result will be unclear problems, even with a proper event name

Status	Info	Host	Problem	Timestamp	Value
PROBLEM		mysql.server.example	Error in the MySQL log file	2025-09-15 11:13:47 AM	Error code: 1064
				2025-09-15 11:13:41 AM	Error code: 1045
				2025-09-15 11:13:37 AM	Error code: 1114
PROBLEM		SNMP Device	SNMP trap contains failure	2025-09-15 11:13:30 AM	Error code: 2006
PROBLEM		SNMP Device	SNMP trap contains Down (DEV-01 (DEV-01/MICRO), Peer: 127.0.0.1 (DEV-01/MICRO))		

Diferrent error codes

Log/snmptrap missteps

Creating a trigger for every single possible error:

- find(/host/log[/var/log/messages,"error"],10m,"like","1064")=1
- find(/host/log[/var/log/messages,"error"],10m,"like","1045")=1
- find(/host/log[/var/log/messages,"error"],10m,"like","1114")=1
- etc.

Items	Triggers
Items 85	Triggers 85
Items 893	Triggers 887
Items 149	Triggers 149
Items 598	Triggers 598
Items 1712	Triggers 1584

The result will be clear problems, with hard to manage configuration

Number of hosts (enabled/disabled)	2970	2969 / 1
Number of templates	194	
Number of items (enabled/disabled/not supported)	2629318	2505537 / 1710 / 122071
Number of triggers (enabled/disabled [problem/ok])	2174988	2158201 / 16787 [926 / 2157275]

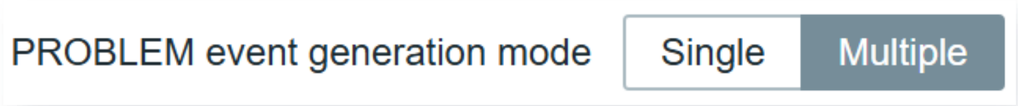
3000 hosts

2 million triggers!

Solution - problem based on value

Use multiple problem event generation:

- One item to collect erroneous data
  - snmptrap.fallback
- One trigger to detect problems
  - find(/host/snmptrap.fallback,,,"raise")=1
- Enable



- "Enjoy" the easy-to-understand problems

Status	Info	Host	Problem
PROBLEM		SNMP Device	SNMP trap contains Down (Rebooted: 91.205.14.178 (PROD-01/MACRO))
PROBLEM		SNMP Device	SNMP trap contains Down (DEV-25, Peer: 68.142.201.33 (DEV-25/MACRO))

- How to resolve those individually?

ZABBIX SUMMIT

OCTOBER 8 · 10, 2025
RIGA · LATVIA

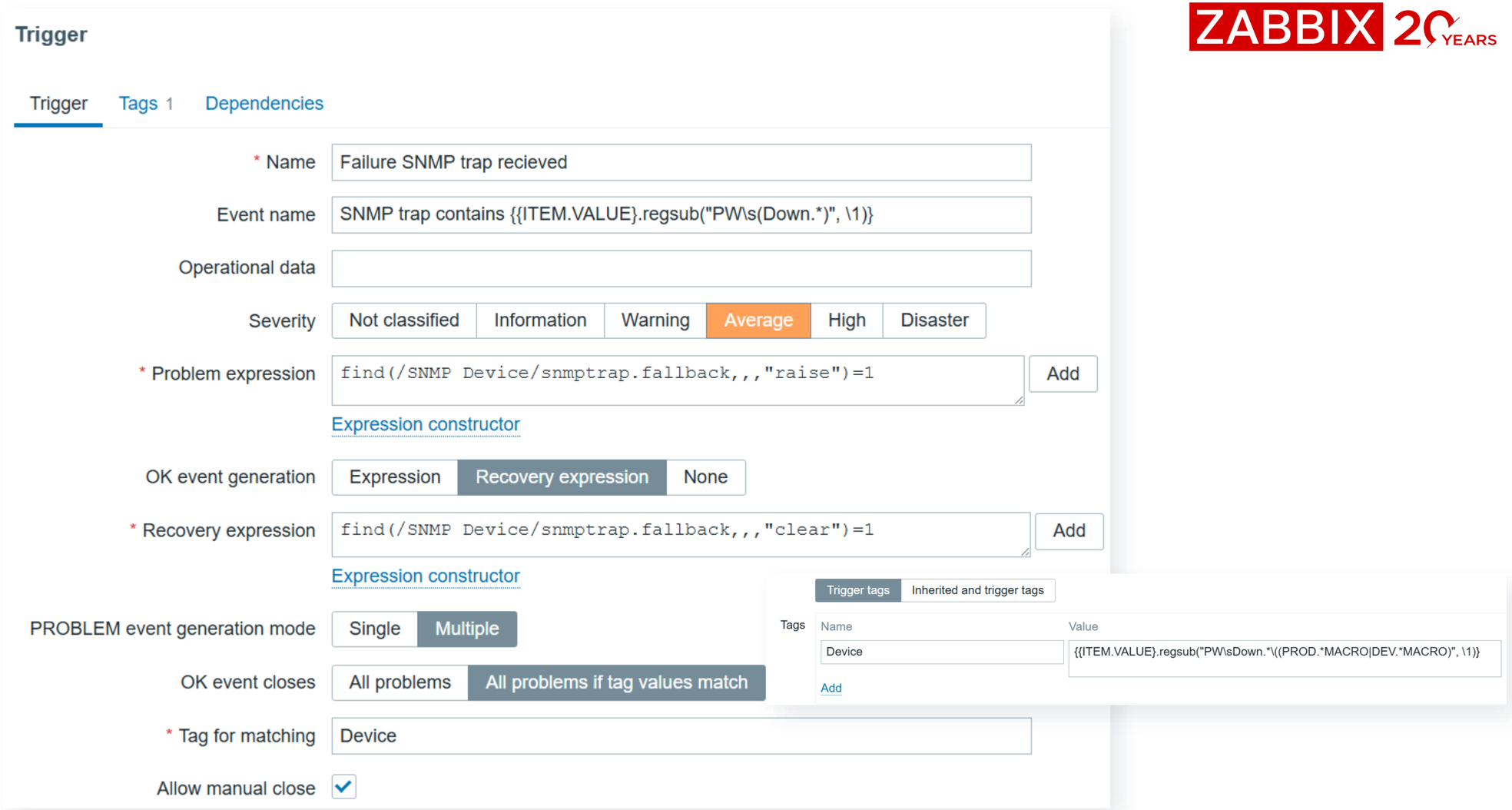
TRIGGER-BASED EVENT CORRELATION

Correlate problems reported by one trigger

Use the power of tags and macro functions

- Extract values with regex to identify problems
  - Host names
  - IPs
  - Error codes
  - OID

- Match problem value with recovery value
  - Best for logs and SNMPTraps
  - Precise correlation
  - One trigger to rule them all

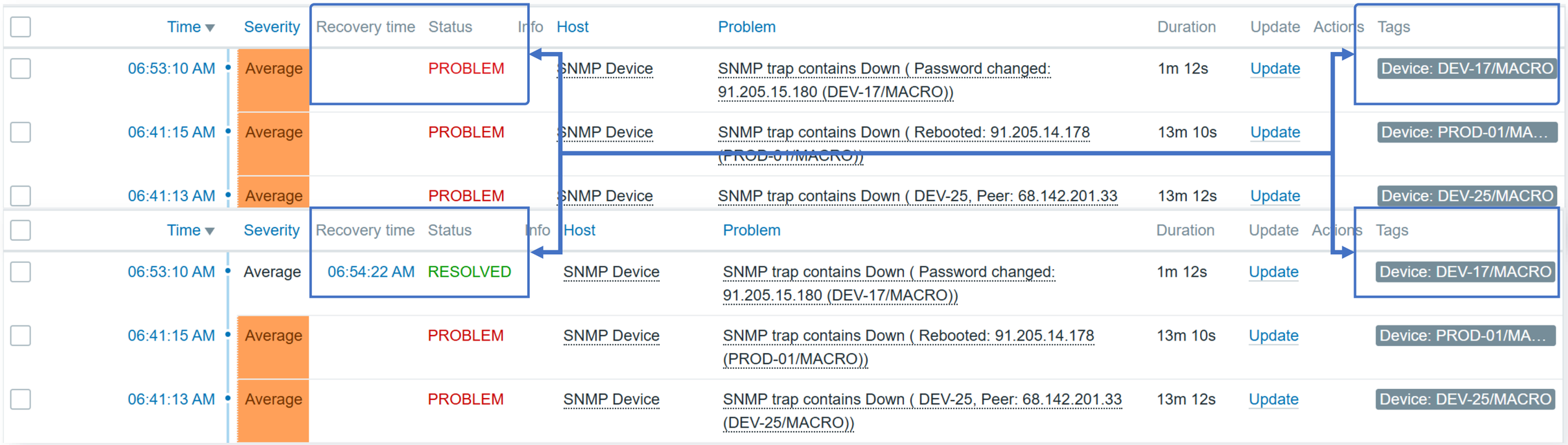


The configuration

The result

Problems with related information will be resolved

- Problem event tags must match recovery event tags
- Remaining problems will remain active



Time	Severity	Recovery time	Status	Info	Host	Problem	Duration	Update	Actions	Tags
06:53:10 AM	Average		PROBLEM		SNMP Device	SNMP trap contains Down (Password changed: 91.205.15.180 (DEV-17/MACRO))	1m 12s	Update		Device: DEV-17/MACRO
06:41:15 AM	Average		PROBLEM		SNMP Device	SNMP trap contains Down (Rebooted: 91.205.14.178 (PROD-01/MACRO))	13m 10s	Update		Device: PROD-01/MA…
06:41:13 AM	Average		PROBLEM		SNMP Device	SNMP trap contains Down (DEV-25, Peer: 68.142.201.33	13m 12s	Update		Device: DEV-25/MACRO

Time	Severity	Recovery time	Status	Info	Host	Problem	Duration	Update	Actions	Tags
06:53:10 AM	Average	06:54:22 AM	RESOLVED		SNMP Device	SNMP trap contains Down (Password changed: 91.205.15.180 (DEV-17/MACRO))	1m 12s	Update		Device: DEV-17/MACRO
06:41:15 AM	Average		PROBLEM		SNMP Device	SNMP trap contains Down (Rebooted: 91.205.14.178 (PROD-01/MACRO))	13m 10s	Update		Device: PROD-01/MA…
06:41:13 AM	Average		PROBLEM		SNMP Device	SNMP trap contains Down (DEV-25, Peer: 68.142.201.33 (DEV-25/MACRO))	13m 12s	Update		Device: DEV-25/MACRO

ZABBIX SUMMIT
OCTOBER 8 · 10, 2025
RIGA · LATVIA

Advanced functions

Less history - more data

To evaluate days/months/years of data we can use:

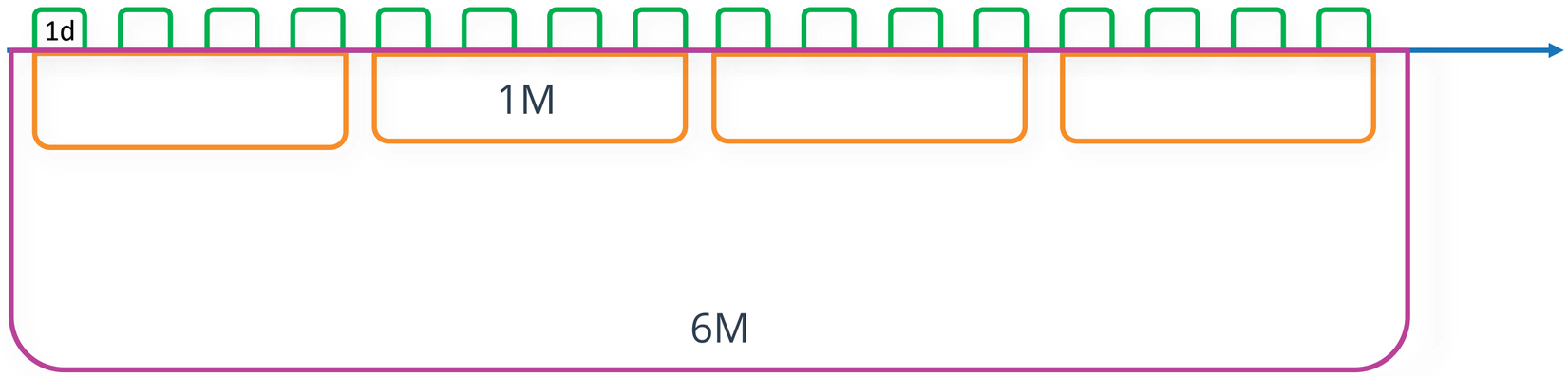
- Trend functions
  - trendfunction(/host/item,period,period_shift)
  - {?trendavg(/Linux server/proc.num, 1M,now/M-1y)}
- All trend functions use data from trends table:
  - Data in trends table must exist for previous periods
  - Current hour is not included in statistics
  - Less memory used comparing to history functions

{?avg(/Linux server/proc.num, 1d)}
on average 300 values

{?trendavg(/Linux server/proc.num, 1d, now/d)}
only 24 values

Use trends to detect anomalies

- baselinewma(/datacenter/cable.light, 1d, 1M, 6M)
  - /datacenter/cable.light key for light intensity in optical cables
  - 1d → aggregating light intensity per day
  - 1M → one season is a full calendar month
  - 6M → compares across the last 6 months
- Calculates moving average baseline of daily light transmission trends, averaged across months.



Menu entry name and URL

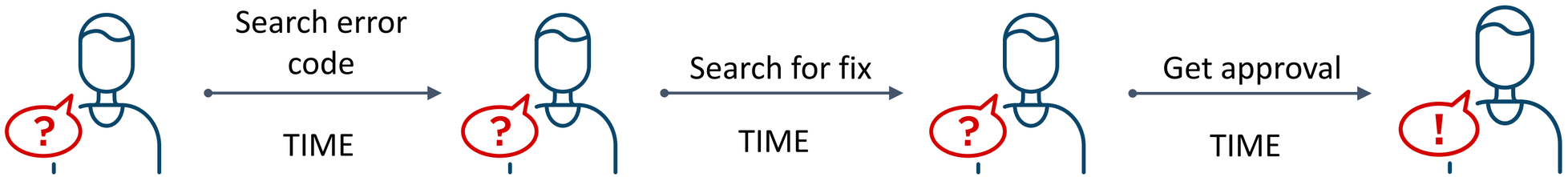
ZABBIX SUMMIT
OCTOBER 8 · 10, 2025
RIGA · LATVIA

Improving resolution time

Problem without menu entry name and link

Severity	Recovery time	Status	Info	Host	Problem
Average		PROBLEM		My Application	Error 2013 in the log file

Problem solving process:



Improving resolution time

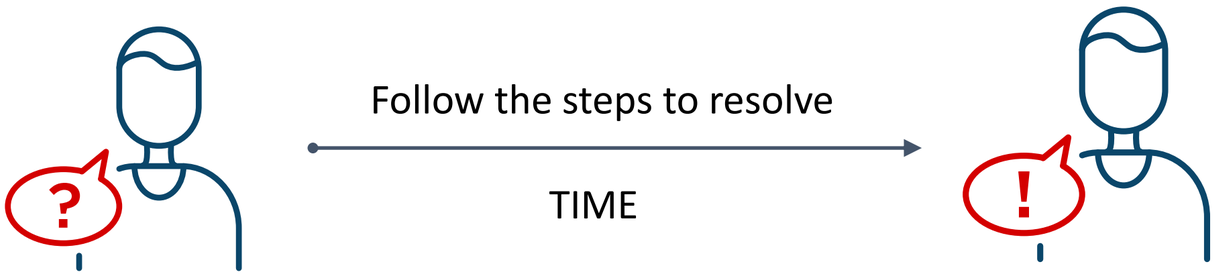
Problem with menu entry name and link

Severity	Recovery time	Status	Info	Host	Problem
Average		PROBLEM		My Application	Error 2013 in the log file

LINKS

Confluence page

Problem solving process:



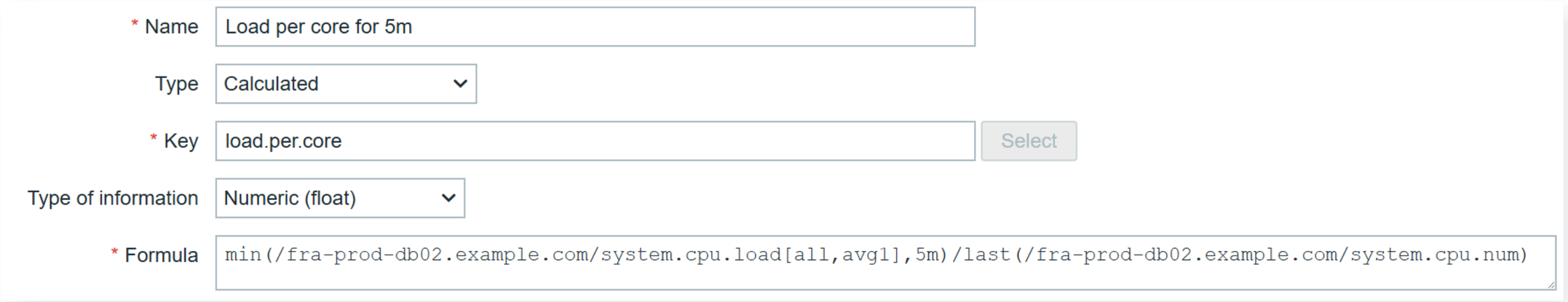
ZABBIX SUMMIT
OCTOBER 8 · 10, 2025
RIGA · LATVIA

Extra hints

Calculated items triggers

Function is complicated?

- Create a calculated item
- Use a graph to visualize it
- Use the calculated item key to build the trigger



Update the template default

You know your environment best

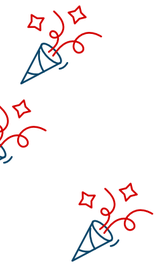
- Create a host
- Link out-of-the-box template
- Adjust the thresholds (macro values)

Macro	Value	Description	
{$MYSQL.ABORTED_CONN.MAX.WARN}	3	Number of failed attempts to connect to the MySQL server for trigger expressions.	Remove
{$MYSQL.BUFF_UTIL.MIN.WARN}	50	The minimum buffer pool utilization in percentage for trigger expressions.	Remove
{$MYSQL.CREATED_TMP_DISK_TABLES.MAX.WARN}	10	The maximum number of temporary tables created on a disk per second for trigger expressions.	Remove
{$MYSQL.CREATED_TMP_FILES.MAX.WARN}	10	The maximum number of temporary files created on a disk per second for trigger expressions.	Remove
{$MYSQL.CREATED_TMP_TABLES.MAX.WARN}	30	The maximum number of temporary tables created in memory per second for trigger expressions.	Remove

Let functions function

Use functions with a reasonable amount of values

- nodata(5m);
- min(3600);
- trendavg(1M)



- nodata(5m) + mult. event generation;
- min(#3600)
- avg(1M)

Mind the cache

Tune Zabbix server value cache:

- Running out of value cache may seriously degrade Zabbix performance
- The same may happen running from trend function cache
- Zabbix will detect issues with value cache and create a problem
- Increase the value cache size and restart Zabbix server

```
### Option: ValueCacheSize
#       Size of history value cache, in bytes.
# Range: 0,128K-64G
ValueCacheSize=16M
```

```
### Option: TrendFunctionCacheSize
#       Size of trend function cache, in bytes.
# Range: 128K-2G
TrendFunctionCacheSize=4M
```

Follow the Matrix

- Does it reflect a real service or business impact?
- Are thresholds defined with hysteresis and severity in mind?
- Does it use aggregation or time-windowed functions (not just last) or no data?
- Does it recover correctly without flapping?
- Are recovery expressions/dependencies set to avoid noise?
- Are tags applied for filtering, integrations, and correllation?
- Is it documented and understandable?

Workshop

15:00 60 m	**Reducing Alert Noise by Choosing Appropriate Trigger Functions and Defining Recovery Expressions**	Aleksandrs Petrovs-Gavrilovs, Zabbix Trainer, Zabbix	Alfa	Technical	Read more

We'll guide you thorough various scenario of trigger tuning, including:

- Aggregation functions
- Percentile
- Trigger level SNMPTrap correlation

You must bring your own laptop to the workshop:

- Individual virtual machines will be provided by Zabbix

THANK YOU!

ZABBIX SUMMIT

OCTOBER 8 · 10, 2025
RIGA · LATVIA