SPRACOVANIE SNMP TRAPOV V ZABBIXE

Marec 2023

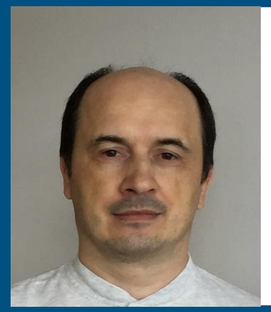
Stanislav Ťažiar

S&T CEE HOLDING

Zabbix premium partner since 2017

The only company in Slovakia

CONTACT US



STANISLAV ŤAŽIAR

CONSULTANT SENIOR

ZABBIX CERTIFIED PROFESSIONAL

Mobil: +421 905 210 301

E-mail: stanislav.taziar@snt.sk

Web: https://www.snt.sk/zabbix.html

Trainings and exams: https://www.snt.sk/zabbix.skolenia.html

Webinars: https://www.snt.sk/zabbix.webinare.html

OBSAH WEBINÁRA

Monitoring SNMP trapov v Zabbixe a metódy ich spracovania

1. Čo sa nám páči/nepáči na SNMP trapoch
2. Základná konfigurácia dohľadu SNMP trapov
3. Konfigurácia pre efektívne riadenie problémov
4. Čo je potrebné riešiť mimo Zabbix
5. Aké riešenie vieme poskytnúť my
6. Vaše otázky

SNMP TRAPY

- Široké uplatnenie SNMP
- Nie je potrebné nasadiť agenta
- Okamžité alarmy

SNMP TRAPY

- ✓ Široké uplatnenie SNMP
- ✓ Nie je potrebné nasadiť agenta
- ✓ Okamžité alarmy

- ☹ Neregulované množstvo dát
- ☹ Nezaručené doručenie (UDP)
- ☹ Nedostatočná dokumentácia

ZABBIX KONCEPT PRE SNMP TRAPY

1. snmptrapd
2. SNMPTT (Perl trap receiver)
3. SNMPTrapperFile
4. Zabbix SNMP trapper
5. Host SNMP interface
6. Item - snmptrap[regexp]
7. Zabbix trigger

ZÁKLADNÁ KONFIGURÁCIA

snmptrapd

snmptrapd.conf

traphandle default /usr/sbin/snmptthandler

ZÁKLADNÁ KONFIGURÁCIA

SNMPTT

snmptt.ini

net_snmp_perl_enable = 1

log_enable = 1

log_file = [TRAP FILE]

date_time_format = [DATE TIME FORMAT]

ZÁKLADNÁ KONFIGURÁCIA

SNMPTrapperFile

↑

Zabbix SNMP trapper

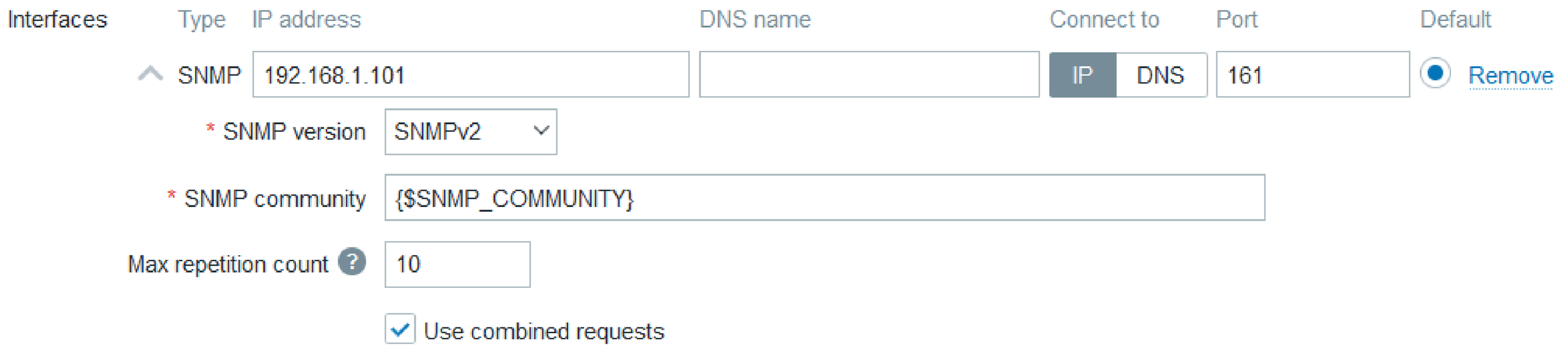
zabbix_proxy.conf

StartSNMPTrapper=1

SNMPTrapperFile=[TRAP FILE]

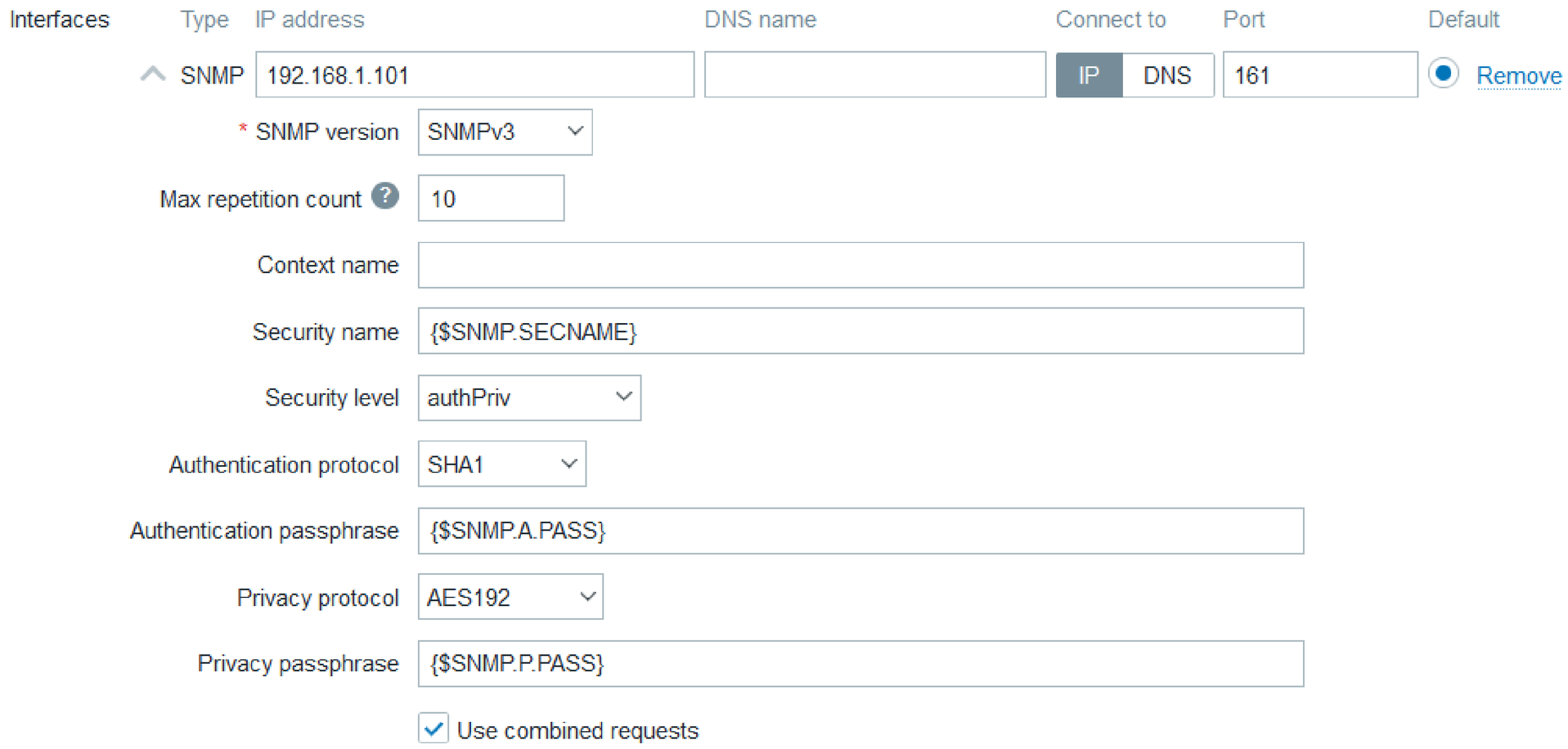
ZÁKLADNÁ KONFIGURÁCIA

Host SNMP interface



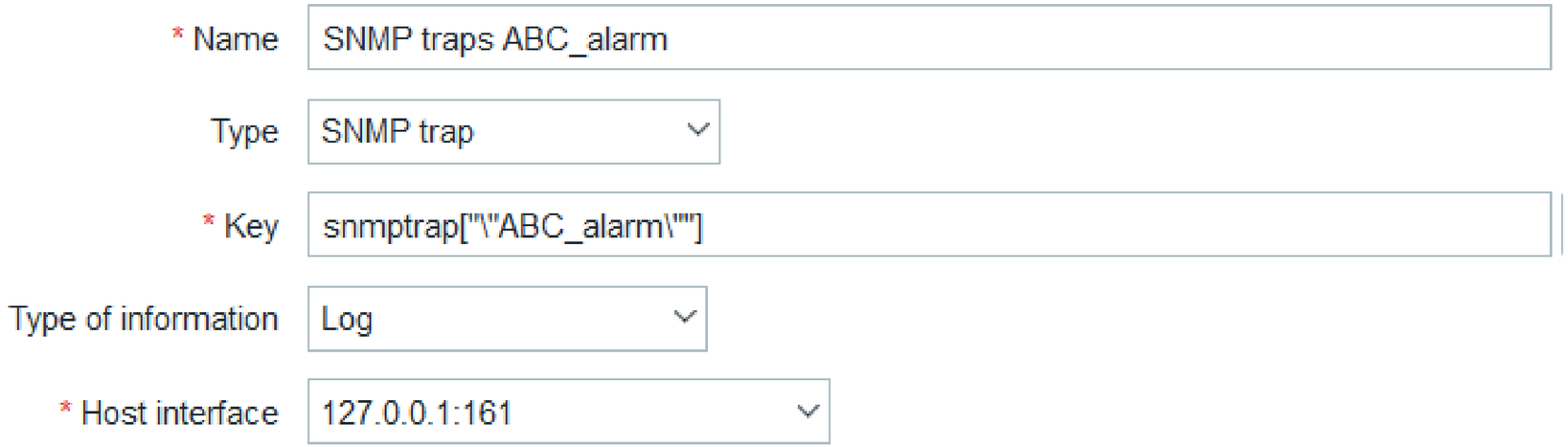
ZÁKLADNÁ KONFIGURÁCIA

Host SNMPv3 interface



ZÁKLADNÁ KONFIGURÁCIA

Zabbix item



SNMPTT.conf

EVENT ABC_alarm .1.3.6.1.4.1.12345.0.2 „ABC_alarm" Normal
FORMAT ZBXTRAP $A $R ABC_trap_data $*

ZÁKLADNÁ KONFIGURÁCIA

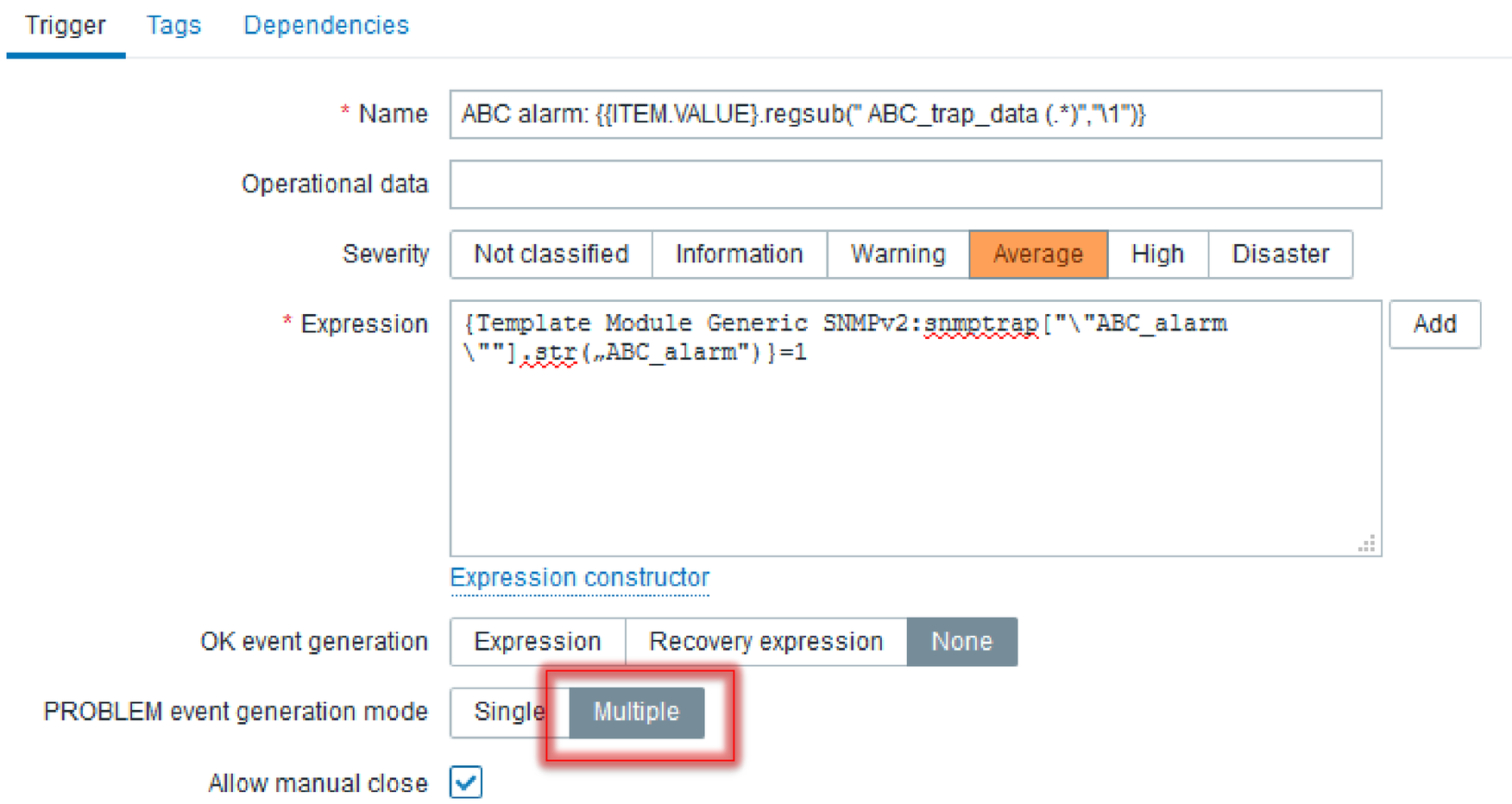
Zabbix trigger

Trigger | Tags | Dependencies

* Name	ABC alarm: {{ITEM.VALUE}.regsub(" ABC_trap_data (.*)","\1")}
Operational data	
Severity	Not classified / Information / Warning / **Average** / High / Disaster
* Expression	{Template Module Generic SNMPv2:snmptrap["\"ABC_alarm \""],str(„ABC_alarm")}=1 [Add]
	Expression constructor
OK event generation	Expression / Recovery expression / **None**
PROBLEM event generation mode	Single / **Multiple**
Allow manual close	☑

ZÁKLADNÁ KONFIGURÁCIA

Zabbix trigger

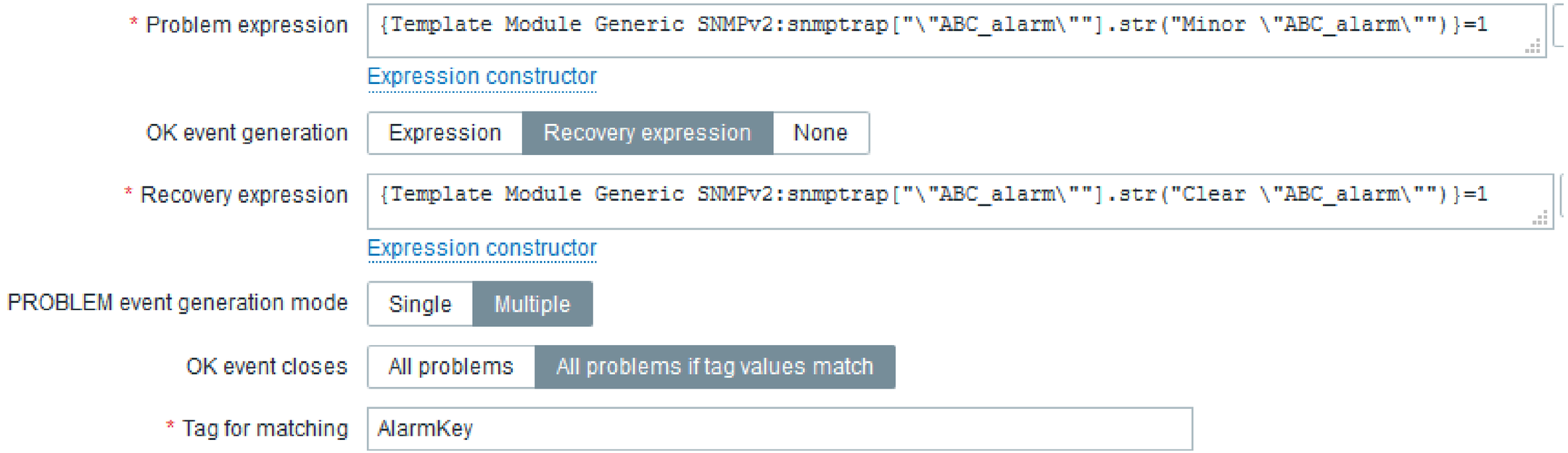


A ČO RIADENIE PROBLÉMOV?

- Clear trapy
- Zmena severity trapu
- Opakovanie trapu

ZATVÁRANIE PROBLÉMOV

- Recovery expression
- Tag for matching



ZATVÁRANIE PROBLÉMOV

Event Correlation

Correlation | Operations

* Name: SNMP traps closing

Type of calculation: And/Or — A and B and C

* Conditions

Label	Name	Action
A	Old event tag name equals *Correlation*	Remove
B	New event tag name equals *Correlation*	Remove
C	Value of old event tag *AlarmKey* equals value of new event tag *AlarmKeyToClose*	Remove

Add

Description: Zavrie SNMP alarmy s urcenym AlarmKey

Correlation | Operations

Close old events: ☑

Close new event: ☐

ZATVÁRANIE PROBLÉMOV

- AlarmKey a AlarmKeyToClose je potrebné správne nastaviť
- Môžu obsahovať OID, VarBinds
- Event Correlation pravidlo stačí jedno globálne
- Toto jedno pravidlo dokáže zatvoriť problem vo viacerých situáciách:
  - CLEAR trap
  - Duplicitný trap – deduplikácia
  - Zmena severity trapu

S ČÍM POMÔŽE SNMPTT

- Filtrovať iba požadované trapy (MATCH)
- Stačí zapisovať iba požadované data/varbindy ($1 $2 …)
- Údaje možno rozšíriť o statické alebo odvodené hodnoty
- Umožňuje predspracovať výstupy napr. pomocou REGEX:

  REGEX (State 1)(State UNKNOWN)

  REGEX (State 2)(State ACTIVE)

  REGEX (State 3)(State STANDBY)

KDE UŽ TIETO NÁSTROJE NESTAČIA

- Time based korelácie

KDE UŽ TIETO NÁSTROJE NESTAČIA

- Time based korelácie:
- Korelácia, deduplikácia, suppressing SNMP trapov, vykonávané už na úrovni Zabbix proxy

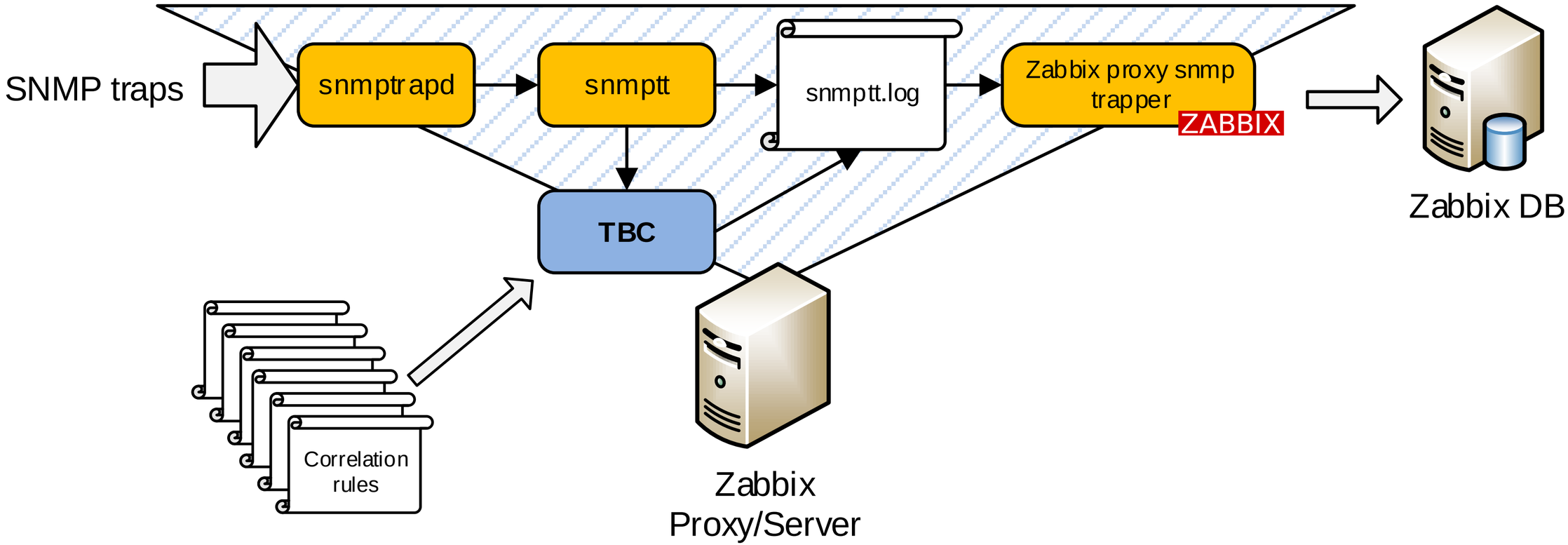
KDE UŽ TIETO NÁSTROJE NESTAČIA

- Time based korelácie:
- Korelácia, deduplikácia, suppressing SNMP trapov, vykonávané už na úrovni Zabbix proxy
- Počítanie duplicít

KDE UŽ TIETO NÁSTROJE NESTAČIA

- Time based korelácie:
- Korelácia, deduplikácia, suppressing SNMP trapov, vykonávané už na úrovni Zabbix proxy
- Počítanie duplicít
- Event storm detection a ochrana pred ním

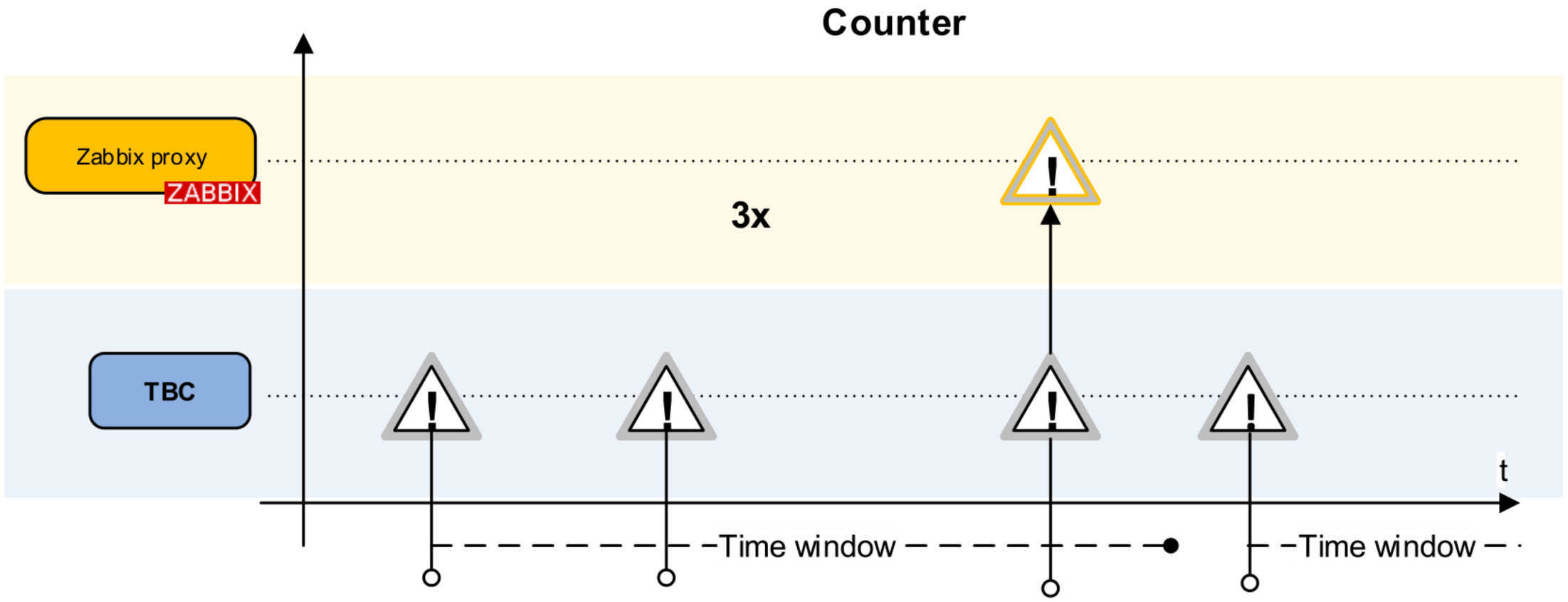
MODUL TBC OD S&T SLOVAKIA



MODUL TBC – PRIPRAVENÉ PRAVIDLÁ

- **Suppress** – potláčanie pomocou podmienok typu white/black list
- **Counter** – prepustenie alarmu po naplnení počtu opakovaní za zvolený čas
- **Timer** – potláčanie opakovaných alarmov po prvom výskyte na zvolený čas
- **Inhibitor** – potláčanie dvojíc alarm/clear
- Spájanie týchto pravidiel do logických celkov
- Možnosť konfigurovať vlastné komplexné korelačné pravidlá
- **Počítanie duplicít** pre všetky pravidlá – informácia v texte problému aj v tagu
- **Postprocessing** udalostí

MODUL TBC – COUNTER



MODUL TBC – COUNTER

Counter 3, 1h

Condition match

<time stamp> <event>

1 CCOUNTER 3 | 81
2 CCOUNTER 3 | 81
3 CCOUNTER 3 | 31 → 3 CCOUNTER 3 | 31
4 CCOUNTER 3 | 435
5 CCOUNTER 3 | 81
6 CCOUNTER 3 | 56 → 6 CCOUNTER 3 | 56

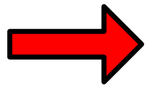
MODUL TBC – COUNTER

Counter 3, 1h

Source match

<time stamp> <event>

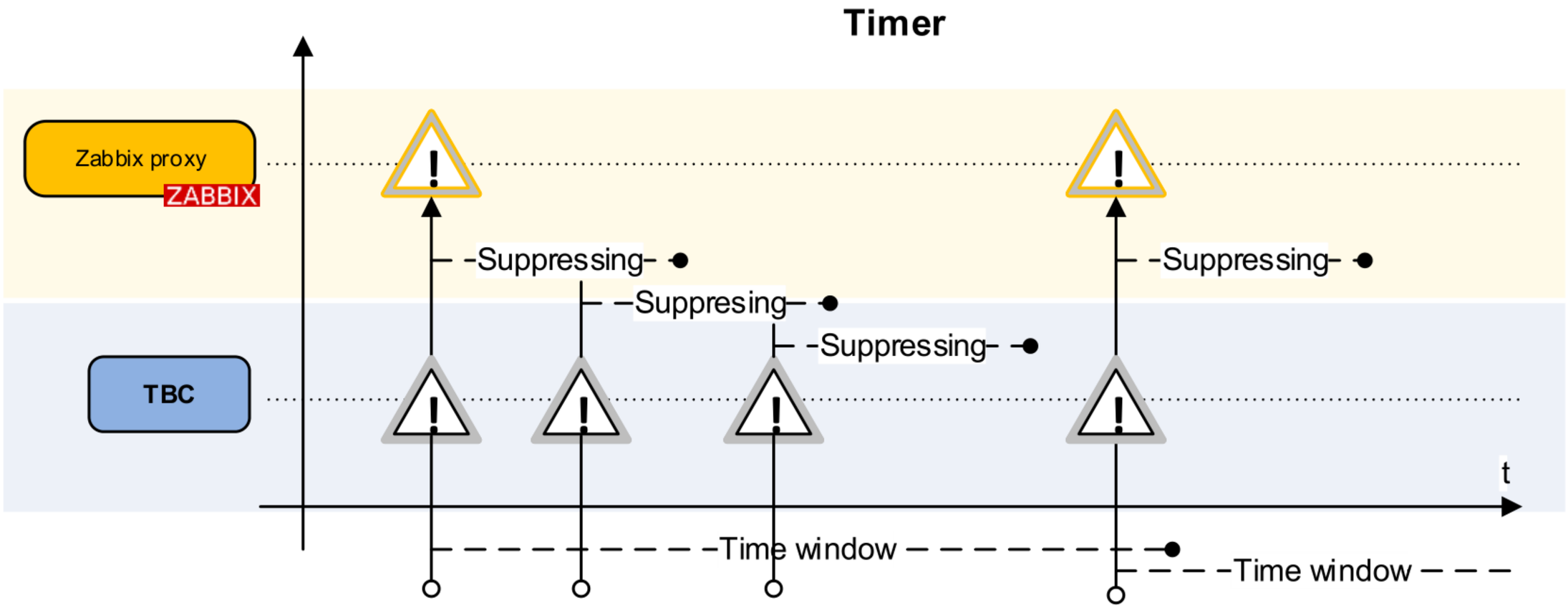
1 SCOUNTER 3 | 81
2 SCOUNTER 3 | 81
3 SCOUNTER 3 | 31
4 SCOUNTER 3 | 435
5 SCOUNTER 3 | 81
6 SCOUNTER 3 | 56



5 SCOUNTER 3 | 81

- Dynamicky vytvárané inštancie pre sledovanie jednotlivých variácií !

MODUL TBC – TIMER

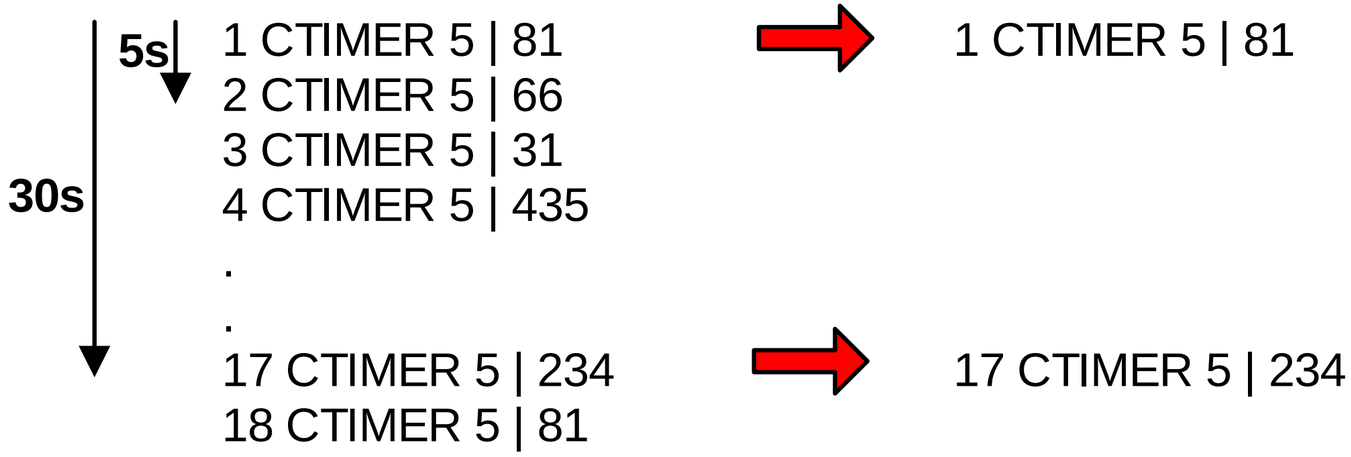


MODUL TBC – TIMER

Timer 5s, 30s

Condition match

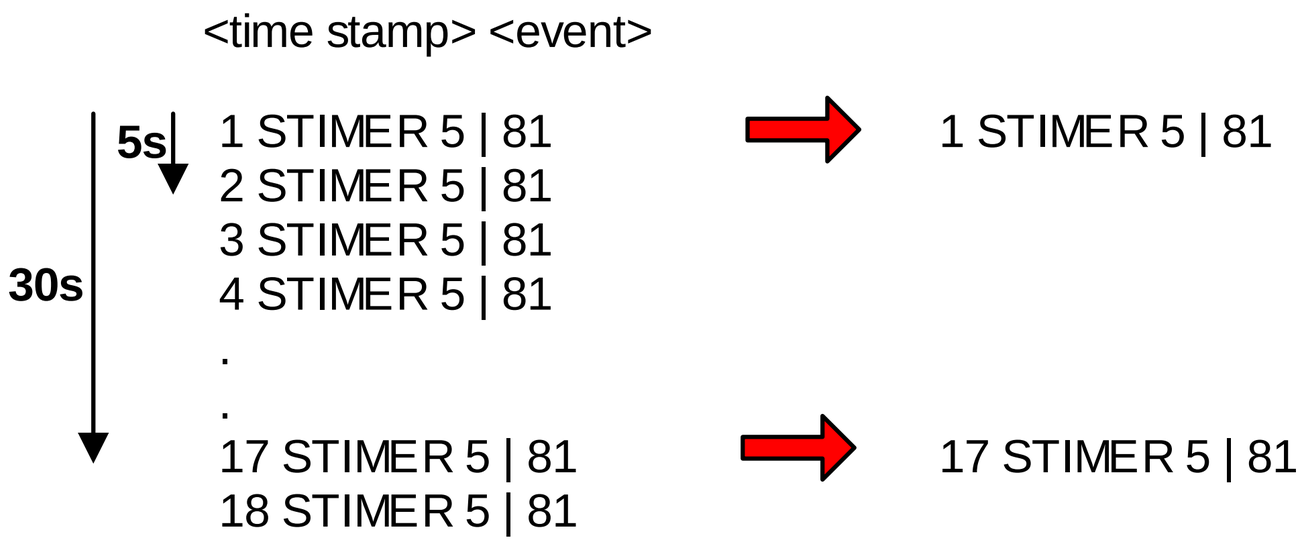
<time stamp> <event>



MODUL TBC – TIMER

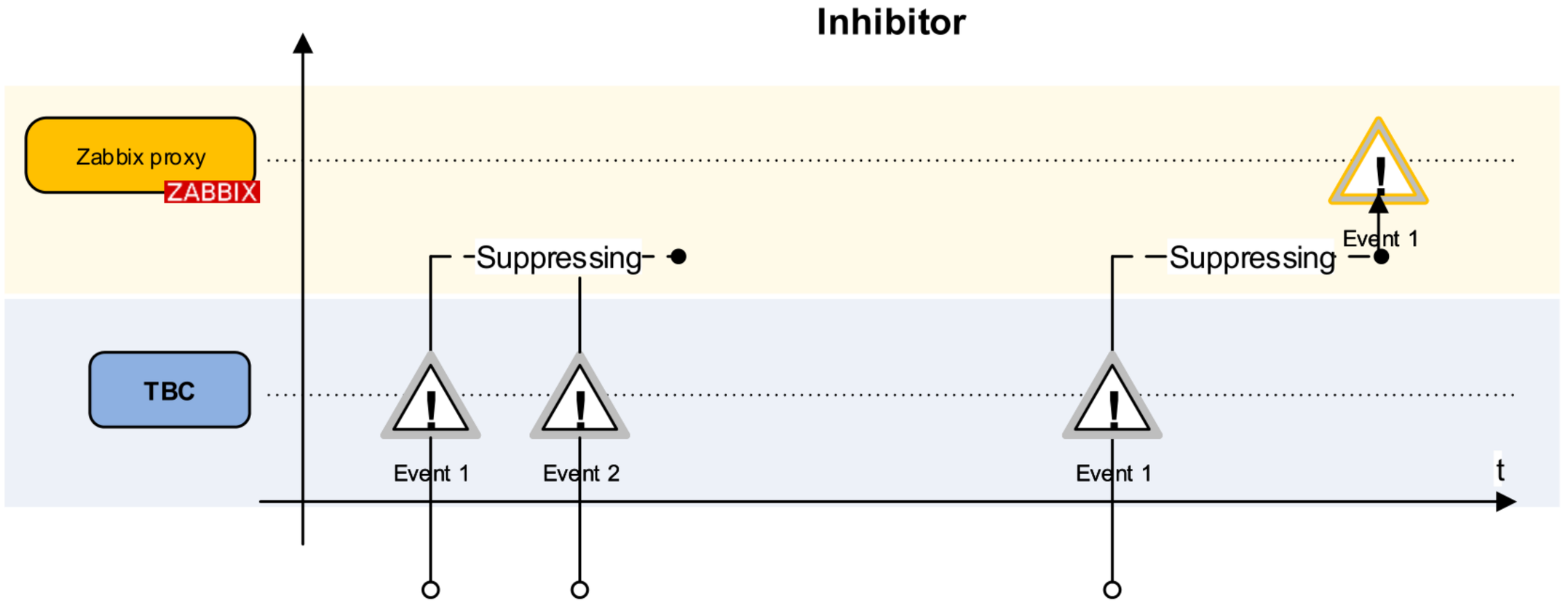
Timer 5s, 30s

Source match



- Dynamicky vytvárané inštancie pre sledovanie jednotlivých variácií !

MODUL TBC – INHIBITOR

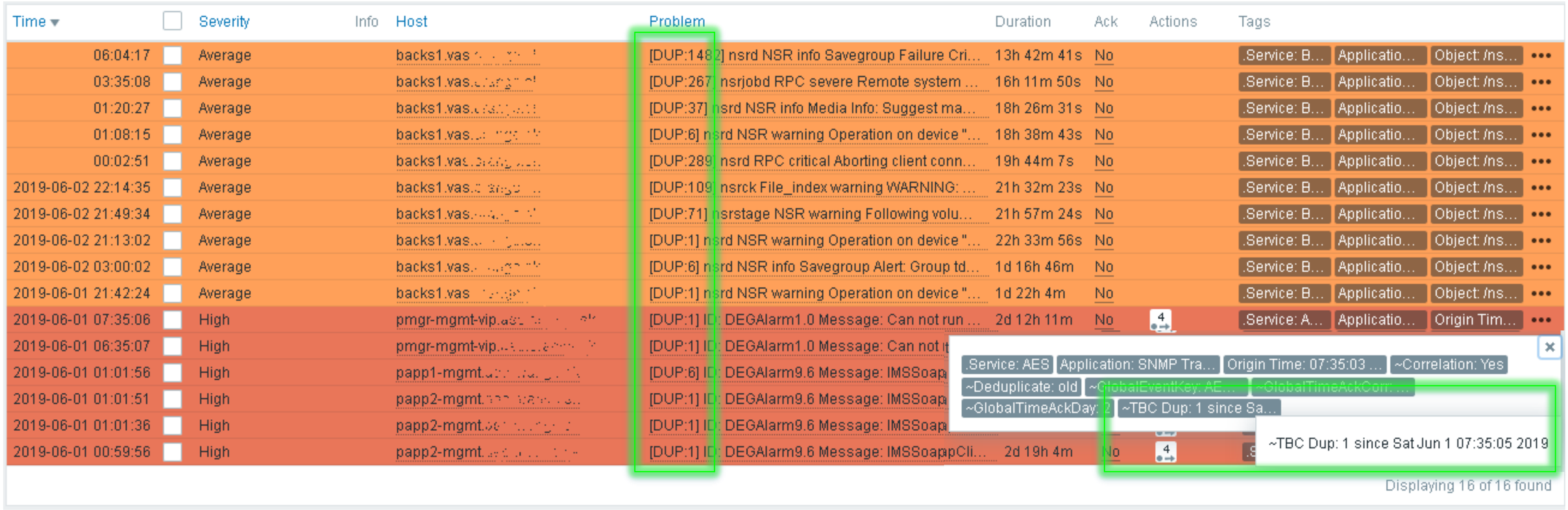


MODUL TBC – POHĽAD

Time		Severity	Info	Host	Problem	Duration	Ack	Actions	Tags
06:04:17		Average		backs1.vas	[DUP:1482] nsrd NSR info Savegroup Failure Cri...	13h 42m 41s	No		Service: B... Applicatio... Object: /ns...
03:35:08		Average		backs1.vas	[DUP:267] nsrjobd RPC severe Remote system ...	16h 11m 50s	No		Service: B... Applicatio... Object: /ns...
01:20:27		Average		backs1.vas	[DUP:37] nsrd NSR info Media Info: Suggest ma...	18h 26m 31s	No		Service: B... Applicatio... Object: /ns...
01:08:15		Average		backs1.vas	[DUP:6] nsrd NSR warning Operation on device "...	18h 38m 43s	No		Service: B... Applicatio... Object: /ns...
00:02:51		Average		backs1.vas	[DUP:289] nsrd RPC critical Aborting client conn...	19h 44m 7s	No		Service: B... Applicatio... Object: /ns...
2019-06-02 22:14:35		Average		backs1.vas	[DUP:109] nsrck File_index warning WARNING: ...	21h 32m 23s	No		Service: B... Applicatio... Object: /ns...
2019-06-02 21:49:34		Average		backs1.vas	[DUP:71] nsrstage NSR warning Following volu...	21h 57m 24s	No		Service: B... Applicatio... Object: /ns...
2019-06-02 21:13:02		Average		backs1.vas	[DUP:1] nsrd NSR warning Operation on device "...	22h 33m 56s	No		Service: B... Applicatio... Object: /ns...
2019-06-02 03:00:02		Average		backs1.vas	[DUP:6] nsrd NSR info Savegroup Alert: Group td...	1d 16h 46m	No		Service: B... Applicatio... Object: /ns...
2019-06-01 21:42:24		Average		backs1.vas	[DUP:1] nsrd NSR warning Operation on device "...	1d 22h 4m	No		Service: B... Applicatio... Object: /ns...
2019-06-01 07:35:06		High		pmgr-mgmt-vip	[DUP:1] ID: DEGAlarm1.0 Message: Can not run ...	2d 12h 11m	No	4	Service: A... Applicatio... Origin Tim...
2019-06-01 06:35:07		High		pmgr-mgmt-vip	[DUP:1] ID: DEGAlarm1.0 Message: Can not run ...	2d 13h 11m	No	4	Service: A... Applicatio... Origin Tim...
2019-06-01 01:01:56		High		papp1-mgmt	[DUP:6] ID: DEGAlarm9.6 Message: IMSSoapCli...	2d 18h 45m	No	4	Service: A... Applicatio... Origin Tim...
2019-06-01 01:01:51		High		papp2-mgmt	[DUP:1] ID: DEGAlarm9.6 Message: IMSSoapCli...	2d 18h 45m	No	4	Service: A... Applicatio... Origin Tim...
2019-06-01 01:01:36		High		papp2-mgmt	[DUP:1] ID: DEGAlarm9.6 Message: IMSSoapCli...	2d 18h 45m	No	4	Service: A... Applicatio... Origin Tim...
2019-06-01 00:59:56		High		papp2-mgmt	[DUP:1] ID: DEGAlarm9.6 Message: IMSSoapCli...	2d 18h 47m	No	4	Service: A... Applicatio... Origin Tim...

Displaying 16 of 16 found

MODUL TBC – POHĽAD



MODUL TBC – STORM DETECTION

- Detekcia nadmerného množstva alarmov z jedného zdroja
- zdroj = označenie trapov v SNMPTT
- Sleduje počet trapov v časovom okne
- Po dosiahnutí stanoveného počtu zastaví odosielanie trapov z tohto zdroja do ZABBIXu a odošle správu
- Ďalej sleduje prichádzajúce trapy
- Po poklese počtu alarmov v časovom okne znovu spustí odosielanie do ZABBIXu

MODUL TBC

- Jadro TBC – jeden skript napísaný v jazyku Perl
- Jediná požiadavka - Perl interpreter
- Nie je potrebná inštalácia žiadnej databázy
- Žiadna Java, ďalšie skripty alebo binárne súbory
- **Self monitoring**
- Pracuje so **SNMP trapmi aj s log súbormi**

Otázky ???

NASLEDUJÚCE WEBINÁRE

12.4.2023
- Korelácie, deduplikácia, tagovanie a vizualizácia udalostí v prostredí Zabbixu

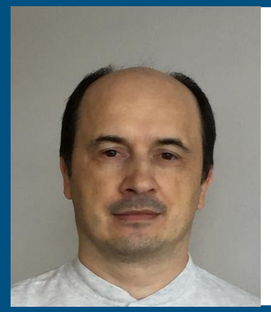
26.4.2023
- Monitoring biznis služieb v prostredí nástroja Zabbix

10.5.2023
- Monitoring cloudových platforiem

24.5.2023
- HA konfiguracia pre Zabbix server

7.6.2023
- Zabbix a riešenie požiadaviek na bezpečný monitoring

CONTACT US



STANISLAV ŤAŽIAR

CONSULTANT SENIOR

ZABBIX CERTIFIED PROFESSIONAL

Mobil: +421 905 210 301

E-mail: stanislav.taziar@snt.sk

Web: https://www.snt.sk/zabbix.html

Trainings and exams: https://www.snt.sk/zabbix.skolenia.html

Webinars: https://www.snt.sk/zabbix.webinare.html

s&t

ZABBIX

PREMIUM PARTNER

Thank you!