TAGOVANIE A KORELÁCIE

Korelácie, deduplikácia, tagovanie a vizualizácia udalostí v prostredí Zabbixu

Marek Konečný
Apríl 2023

KONTAKTUJTE NÁS

MAREK KONEČNÝ

CONSULTANT SENIOR

ZABBIX CERTIFIED TRAINER AND EXPERT

Mobil: +421 905 618 324

E-mail: marek.konecny@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 CEE HOLDING

ZABBIX premium partner

Zabbix premium partner since 2017

The only company in Slovakia

TAGOVANIE A KORELÁCIE

Korelácie, deduplikácia, tagovanie a vizualizácia udalostí v prostredí Zabbixu

Marek Konečný
Apríl 2023

AGENDA

1 **AKO VZNIKLI TAGY**
História

2 **ČO SÚ TAGY**
Definícia tagov a účel ich použitia

3 **PRÍKLADY VYUŽITIA TAGOV**
Kde a ako je možné tagy využiť

4 **KORELÁCIE**
Korelácia na úrovni triggerov a globálna korelácia

5 **ŽIVÉ DEMO**
Príklady využitia tagov pre korelačné účely

1| Čo sú tagy a ako vznikli

ČO SÚ TAGY?

Ako a prečo vznikli

- **Rok 2015** – Orange Slovensko hľadá produkt, ktorý nahradí platené monitorovacie riešenia
- Zabbix 3.0 – jedna z možných náhrad ale s viacerými nedostatkami; chýbajú incidenty, atribúty, korelácie...
- Vzniká partnerstvo Zabbix – S&T a spolupráca na nových funkcionalitách pre Orange Slovensko, vznikajú nové koncepty – tagovanie, korelácie, problémy, filtrovanie...
- **Rok 2016** – vzniká nová verzia **Zabbix 3.2**, Zabbix sa stáva systém management!

ČO SÚ TAGY?

Ako a prečo vznikli

Zabbix 3.2 ako nástroj event managementu:

- Incidenty – entita Zabbix problem
- Tagy – zatial len na úrovni triggerov za účelom konfigurácie atribútov pre Zabbix problems a pre korelačné účely
- Korelačný engine – korelácia na báze tagov
- Prezentačná vrstva – filtrovanie na báze tagov

ČO SÚ TAGY?

Ďalší vývoj

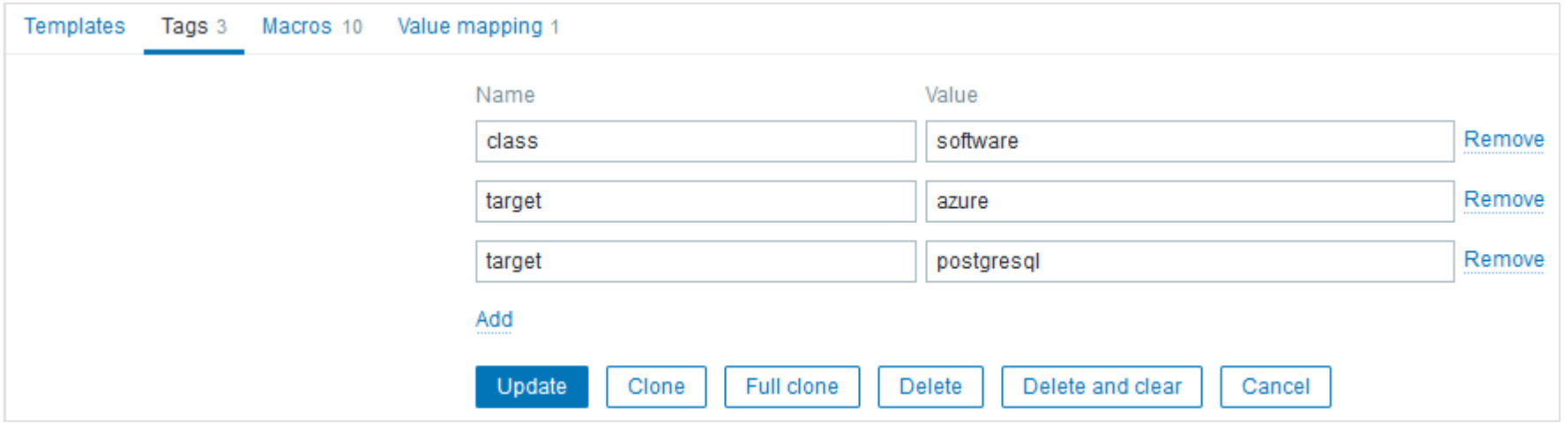
Tagy postupne ovládli celý Zabbix. Tagy je možné v súčasnosti konfigurovať pre množstvo Zabbix entít:

- Šablóny
- Hosty
- Itemy a triggery (na úrovni hosta a šablóny)
- Web scenáre
- Prototypy hostov, itemov a triggerov (na úrovni hosta a šablóny)
- Služby - Services

ČO SÚ TAGY?

Definícia entity tag

Tag je definovaný ako pár Názov: Hodnota



ČO SÚ TAGY?

Účel tagov

- Základný účel – tvorba atribútov pre udalosti/problémy
- Ďalšie použitie:
  - Oprávnenia prístupu k problémom – filtrovanie na báze tagov
  - Akcie – filtrovanie na báze tagov
  - Korelácie – korelačné pravidlá založené na porovnávaní tagov generovaných udalostí
  - Strom služieb – väzba na uzly stromu služieb cez tagy
  - Agregačné funkcie – filtrovanie na báze tagov
  - Maintenance

PREZENTÁCIA TAGOV

Vzťahy medzi tagmi a Zabbix entitami

Pôvod a prezentácia tagov z pohľadu Zabbix usera:

Tag presentation	Tag assigment							
	Item	Trigger	Template	Host	Web	LLD Item	LDD trigger	LLD host
Problem	x	x	x	x	x	x	x	x
Item	x				x	x		
Host			x	x				x

TAGOVANIE UDALOSTÍ/PROBLÉMOV

Použitie makier

- Je možné použiť viacero druhov makier:
  - Build-in makrá **{...}**
  - User makrá **{$...}**
  - LLD makrá **{#...}**
- Makrá je možné použiť pre hodnotu a aj pre názov tagu
- Makrá sú rezolvované len pri vzniku udalosti
- Zhodné kombinácie **Názov: Hodnota** sú prezentované jedným tagom
- **Ak sa makrá líšia v hodnote a zhodujú v názve, vzniká viacero makier s rovnakým názvom – veľmi užitočná funkcionalita pre korelácie!**

TAGOVANIE UDALOSTÍ/PROBLÉMOV

Metodika pomenovania tagov

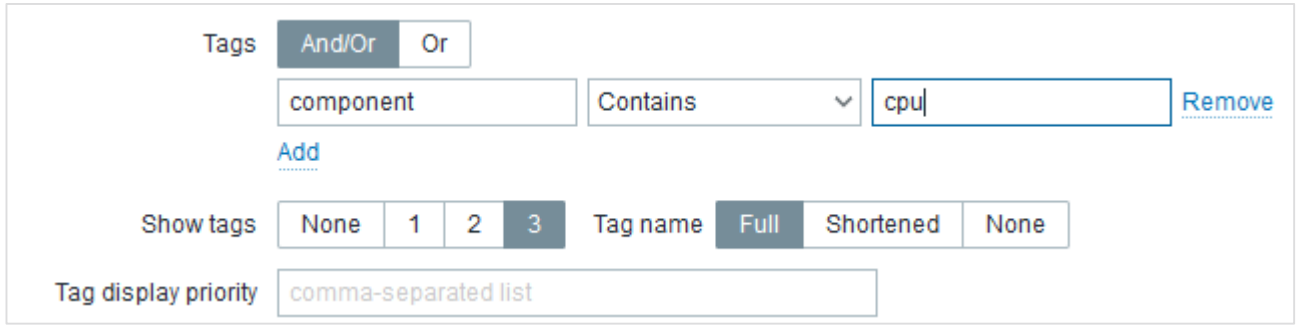
Odporúčania (z praxe) pomenovania tagov:

- **Na úrovni šablón** - označenie účelu šablóny (napr. **DB servers: Oracle**)
- **Na úrovni hostov** - označenie prostredia (napr. **Environment: Production**)
- **Na úrovni itemov** - označenie typu
- **Dot tagy** – významné atribúty zobrazené na prvých miestach
- **Tilda tagy** – skryté atribúty (korelácie, identifikátory, notifikačné príznaky)

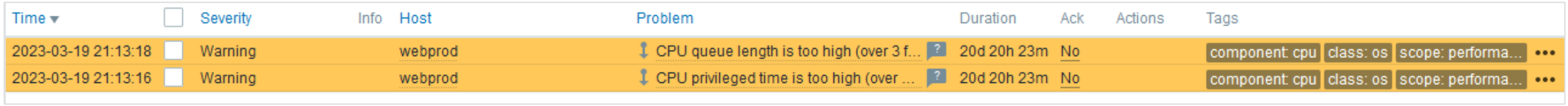
TAGOVANIE UDALOSTÍ/PROBLÉMOV

Použitie filtrovania pomocou tagov

Nastavenie filtra (**Monitoring-> Problems**):



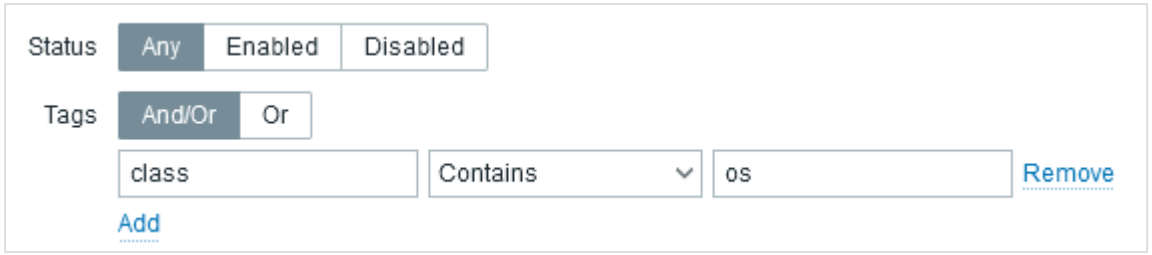
Prezentácia problémov:



TAGOVANIE HOSTOV

Použitie filtrovania pomocou tagov

Nastavenie filtra (**Monitoring -> Hosts**):



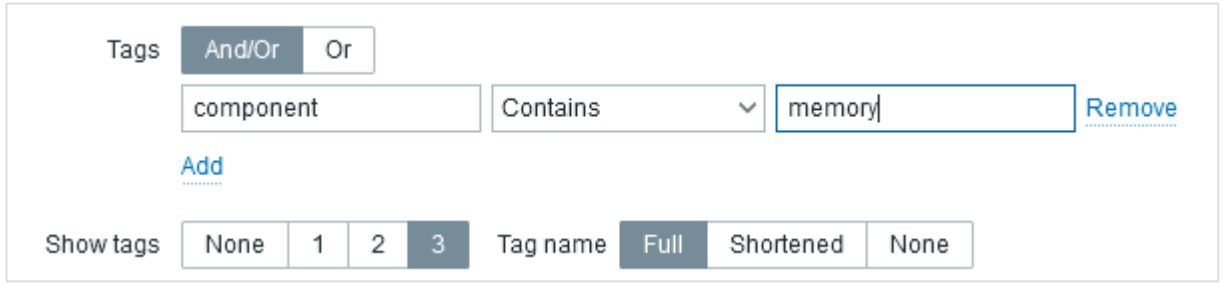
Prezentácia hostov:

[redacted]	ZBX	class: os target: windows	Enabled	Latest data 92	4 1	Graphs 8	Dashboards 1	Web
[redacted]	ZBX	class: os target: windows	Enabled	Latest data 104	Problems	Graphs 11	Dashboards 2	Web
[redacted]	ZBX	class: os target: windows	Enabled	Latest data 116	2	Graphs 16	Dashboards 2	Web

TAGOVANIE ITEMOV

Použitie filtrovania pomocou tagov

Nastavenie filtra (**Monitoring -> Latest data**):



Prezentácia itemov:

Host	Name ▲	Last check	Last value	Change	Tags	Info
[redacted]	Available memory				component: memory	Graph
[redacted]	Available memory in %				component: memory	Graph
[redacted]	Free swap space				component: memory component: storage	Graph

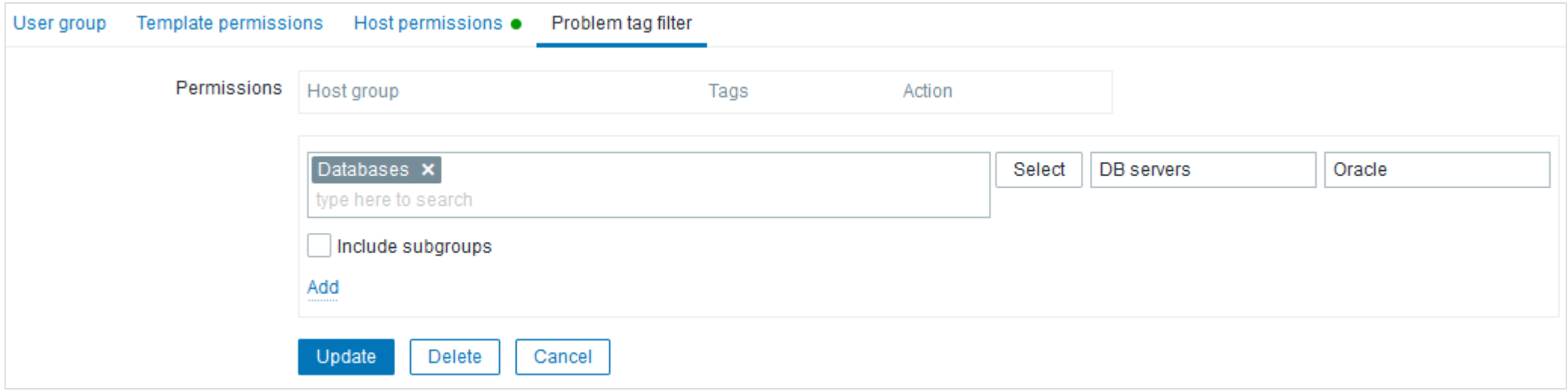
2| Príklady využitia tagov

PRÍKLADY VYUŽITIA TAGOV

Prístup k Zabbix problémom

Limitácia prístupu k problémom:

- Užívateľ vidí problémy z konkrétnej skupiny hostov (Host group) a s konkrétnym tagovaním
- Nastavenie na úrovni skupín užívateľov (**Users -> User groups**)

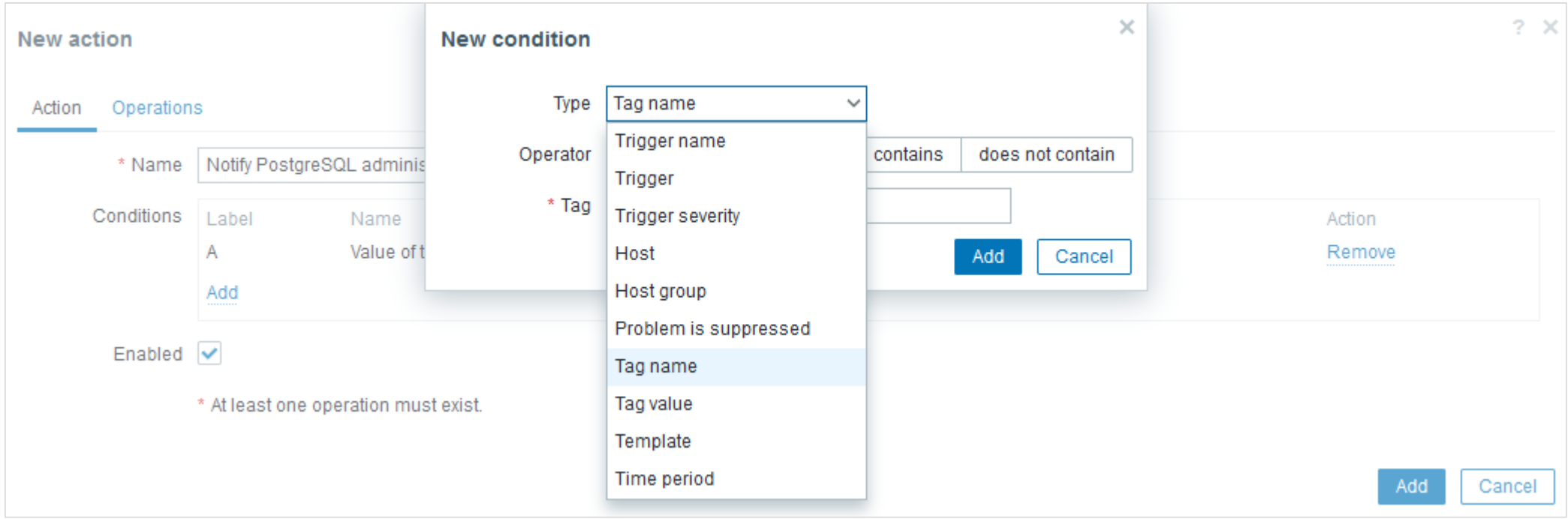


PRÍKLADY VYUŽITIA TAGOV

Automatické akcie

Generovanie notifikácií na základe tagovania Zabbix problémov:

› Konfigurácia akcií pre triggery (**Alerts -> Actions -> Trigger actions**)

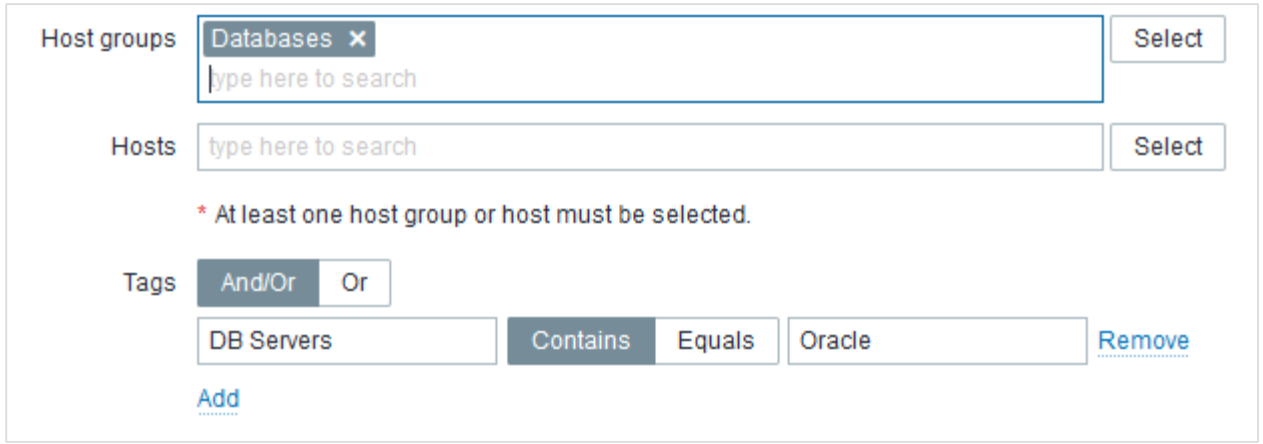


PRÍKLADY VYUŽITIA TAGOV

Maintenance

Potláčanie problémov na báze tagov:

› Konfigurácia maintenance (**Data collection -> Maintenance**)

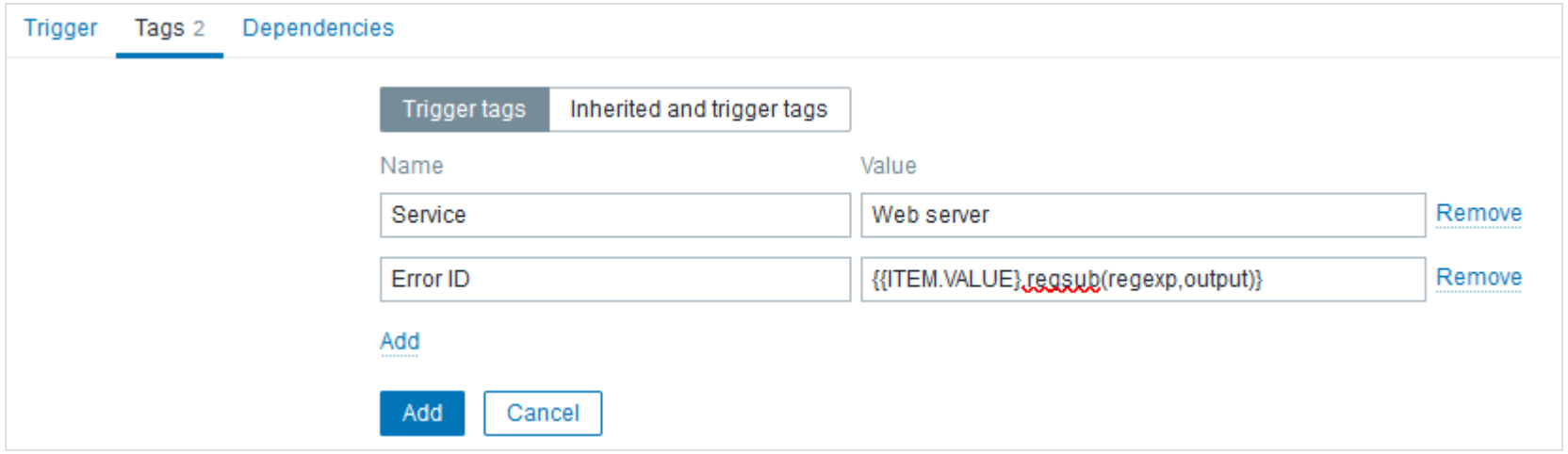


PRÍKLADY VYUŽITIA TAGOV

Extrakcia hodnôt z itemov

Extrahovanie hodnôt z itemov a ich ukladanie ako hodnôt tagov:

- Konfigurácia tagov na úrovni triggerov
- Použitie funkcií regsub alebo iregsub - **{{ITEM.VALUE}.regsub(regexp,output)}**
- **Ponúka široké možnosti pri korelovaní a spracovaní logov, trapov alebo iných zdrojov udalostí!**

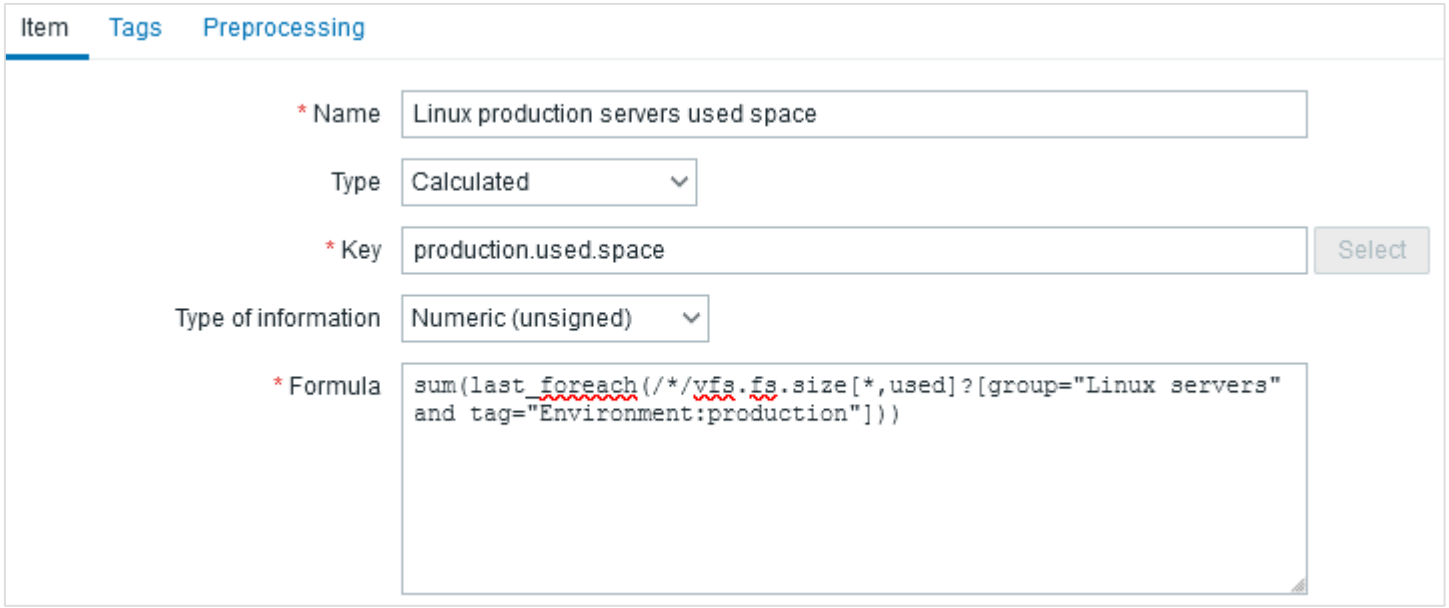


PRÍKLADY VYUŽITIA TAGOV

Agregačné funkcie

Agregovanie itemov na báze tagov:

- Konfigurácia itemov typu Calculated
- Použitie v kalkulačnom vzorci

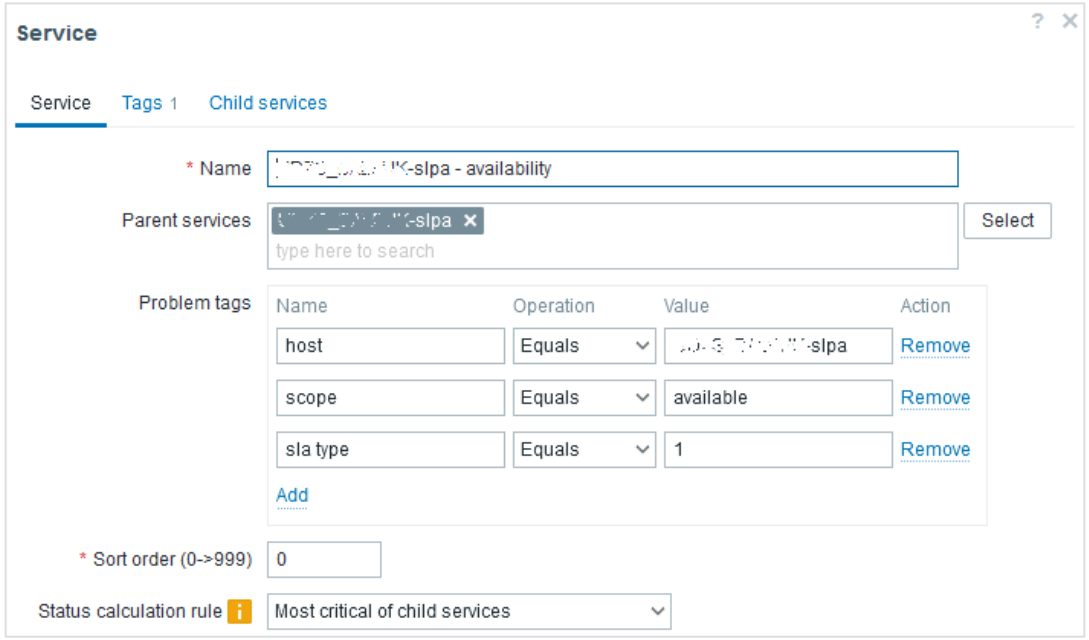


PRÍKLADY VYUŽITIA TAGOV

Services a SLA

Konfigurovanie stromu služieb (**Services -> Services**):

- **S&T BSM modul – funkcionalita prenesená do Zabbixu 6.0**
  - Propagačné a kalkulačné pravidlá
  - Notifikácie pri zmene stavu uzla stromu
  - Vyhodnocovanie SLA
  - **Mapovanie udalostí na uzly stromu pomocou tagov a nie triggerov!**
- Informáciu o incidente nesie udalosť nie trigger
- Samostatný webinár venovaný tejto problematike



3| Korelácie

KORELÁCIE

Vznik a história

Korelácie na úrovni triggerov a globálne korelácie od verzie 3.2 – riešenie požiadaviek spoločnosti Orange Slovensko pri prechode z plateného nástroja na Zabbix:

- **Korelačný engine** – vysoký výkon a priepustnosť
- Fungovanie na základe korelačných pravidiel a tagov
- Automatizované uzatváranie problémov a deduplikácia problémov

KORELÁCIE

Typy korelácií

Dva typy korelácií udalostí:

- **Korelácia na úrovni triggera** – korelácia udalostí generovaných jedným triggerom konfigurovaná na úrovni triggera
- **Globálna korelácia** – korelácia udalostí zo všetkých triggerov na báze globálnych korelačných pravidiel

KORELÁCIE

Korelácia na úrovni triggera

Uzatváranie problémov generovaných jedným triggerom:

- Vybraný tag nesie hodnotu, ktorá odlišuje jednotlivé generované udalosti
- Otvorené problémy sú uzatvárané na základe zhody vybraných tagov a ich hodnôt generovaných udalostí
- Vhodné pre externé zdroje udalostí, log súbory, SNMP trapy...

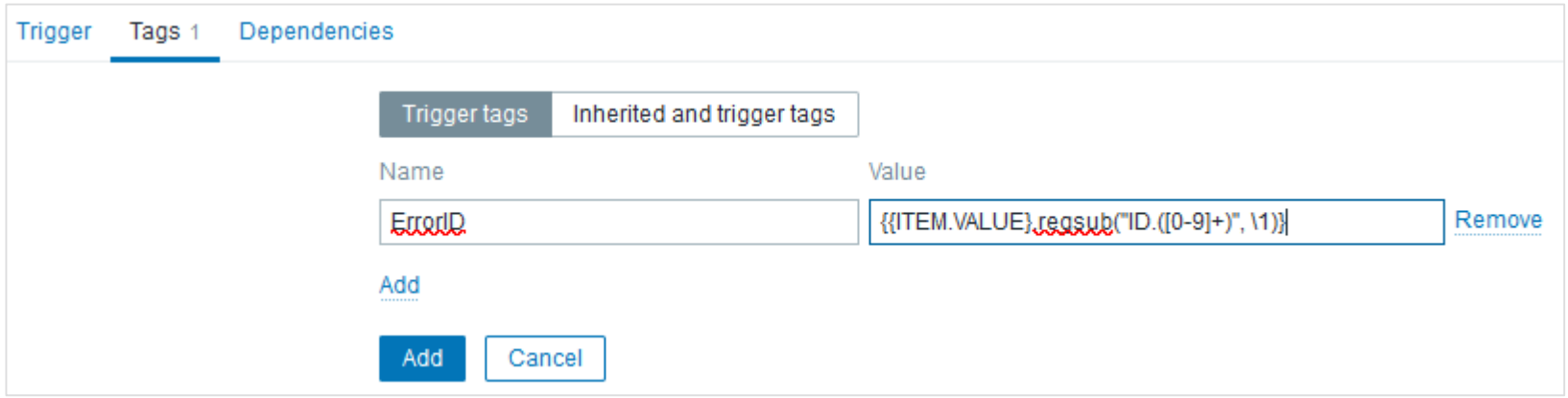
KORELÁCIE

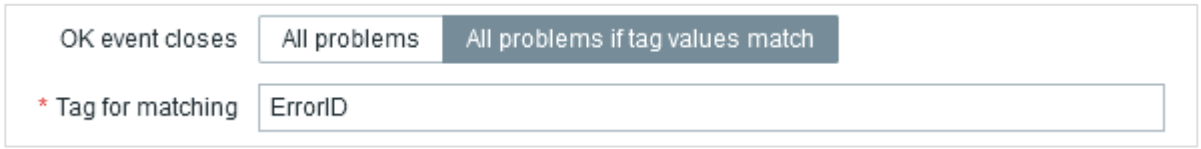
Korelácia na úrovni triggera

Log súbor ako zdroj udalosti:

```
Error ID:123 Event description
```

Vytvorenie triggera s tagom, ktorý identifikuje konkrétny typ udalosti:



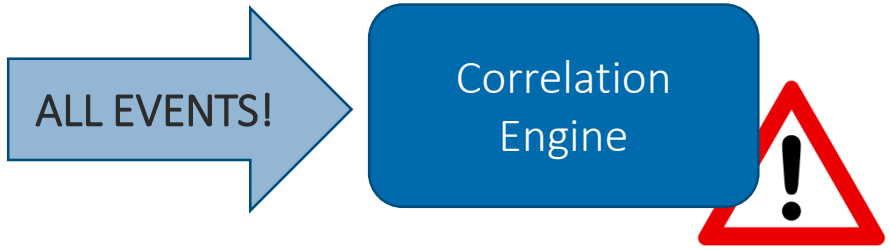


KORELÁCIE

Globálna korelácia

Uzatváranie problémov generovaných všetkými triggermi:

- Korelácia pomocou globálnych **korelačných pravidiel**
- Korelačné pravidlá – komplexné definície názvov tagov, ich hodnôt a ich vzájomných vzťahov medzi práve vygenerovanými udalosťami a už udalosťami vygenerovanými v minulosti
- **Všetky korelačné pravidlá sa vykonávajú nad všetkými udalosťami a definujú, čo sa má stať s už otvorenými problémami a aktuálne generovanými problémami**

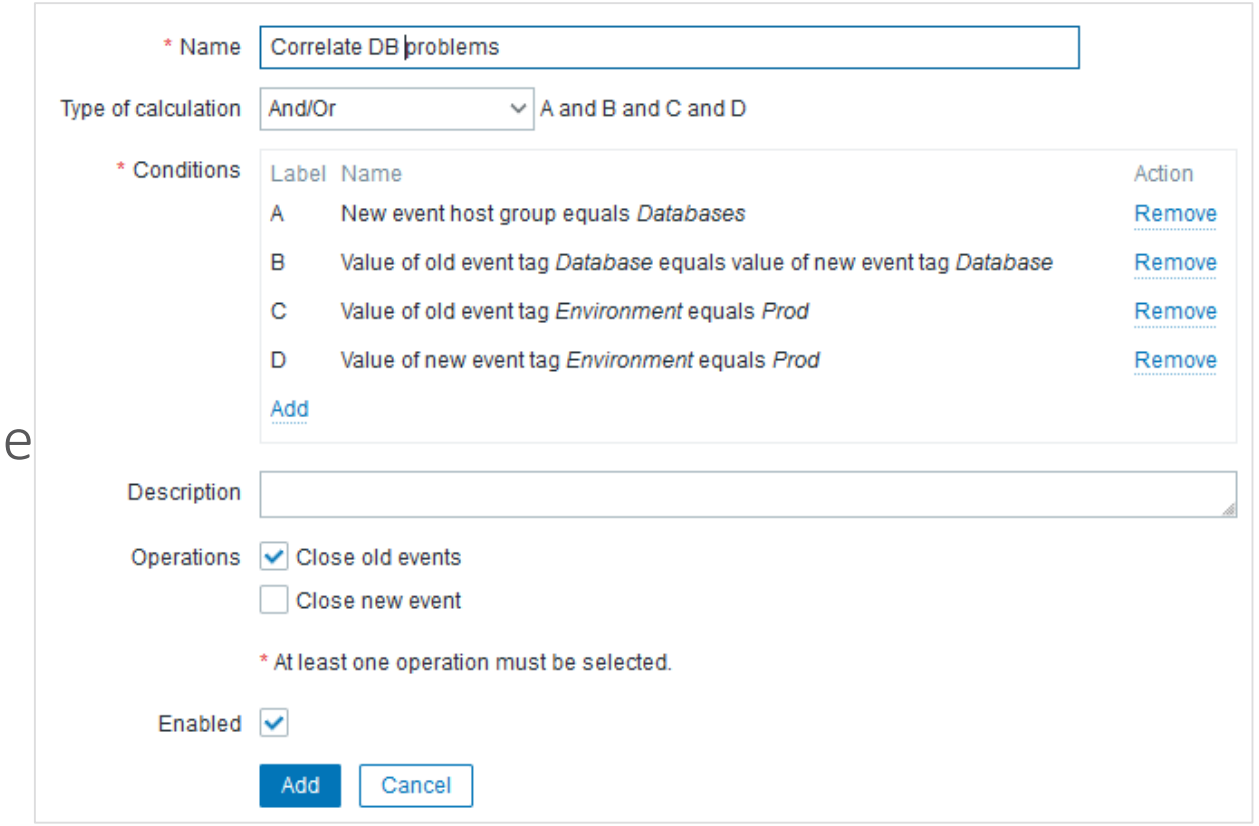


KORELÁCIE

Globálna korelácia

Globálne korelačné pravidlá môže vytvárať len Zabbix super administrator:

- Vytváranie globálnych korelačných pravidiel **Data collection -> Event correlation**
- Operácie definujú čo sa má udiať v prípade platnosti podmienok:
  - **Close old events**
  - **Close new event**



KORELÁCIE

Time Based Correlation – za hranicami možností Zabbixu

Time based korelácie:

- Korelácia, deduplikácia, suppressing vykonávané už na úrovni Zabbix proxy alebo Zabbix agenta pre log súbory, SNMP trapy, databázy...
- Počítanie duplicít
- Event storm detection a ochrana pred ním
- **TBC –** rozšírenie od S&T pre Zabbix postavené na volne dostupnom korelačnom engine SEC (https://github.com/simple-evcorr/sec)

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...

4| Živé demo

ŽIVÉ DEMO

Korelácia na úrovni triggera

Prípad č.1 - korelácia na úrovni triggera:

- Zánam typu **Warning** otvára problém. Záznam typu **Normal** uzatvára problém, ak záznamy majú zhodné atribúty **ID** a **Source**

```
Text:Event description ID:001 Source:A Status:Warning
Text:Event description ID:002 Source:B Status:Warning
Text:Event description ID:002 Source:B Status:Normal
Text:Event description ID:002 Source:C Status:Warning
Text:Event description ID:001 Source:A Status:Normal
```

ŽIVÉ DEMO

Globálna korelácia

Prípad č.2 - globálna korelácia, skupinové zatváranie problémov:

- Každý záznam otvára problém jednoznačne identifikovaný pomocou číselného identifikátora (**vyznačené červenou farbou**) a zároveň uzatvára všetky otvorené problémy identifikované sekvenciou číselných identifikátorov (**vyznačené zelenou farbou**).

```
161649::API server is NOT RUNNING!::161649::No::CRITICAL
161651::API server is NOT RUNNING!::161649::No::WARNING
161652::API server is NOT RUNNING!::161649|161651::No::MAJOR
161650::API server is RUNNING::161650|161649::No::NORMAL
161650::API server is RUNNING::161651|161652|16789::No::NORMAL
```

ŽIVÉ DEMO

Globálna korelácia

Prípad č.2 - globálna korelácia, okamžité uzatváranie problémov so severitou NORMAL/INFORM:

› Udalosť na vstupe so severitou **NORMAL** zabezpečí uzatvorenie všetkých otvorených problémov identifikovaných sekvenciou číselných identifikátorov (**vyznačené zelenou farbou**) a samotný problém so severitou NORMAL sa ihneď uzatvorí

```
161649::API server is NOT RUNNING!::161649::No::CRITICAL
161651::API server is NOT RUNNING!::161649::No::WARNING
161652::API server is NOT RUNNING!::161649|161651::No::MAJOR
161650::API server is RUNNING::161650|161649::No::NORMAL
161650::API server is RUNNING::161651|161652|16789::No::NORMAL
```

ŽIVÉ DEMO
Globálna korelácia

Prípad č.3 - globálna korelácia, deduplikácia:

› Všetky udalosti s rovnakým indetifikátorom (**vyznačené červenou farbou**) sú deduplikované (neotvára sa nový problém, zostáva otvorený problém vygenerovaný pri prvom výskyte udalosti) a to len v prípade, ak je nastavený atribút deduplikácie na hodnotu **Old (uzatvára sa už otvorený problém)** alebo **New (uzatvára sa nový problém)**

```
161649::API server is NOT RUNNING!::161649::No::CRITICAL
161651::API server is NOT RUNNING!::161649::Old::WARNING
161652::API server is NOT RUNNING!::161649|161651::New::MAJOR
161650::API server is RUNNING::161650|161649::Old::NORMAL
161650::API server is RUNNING::161651|161652|16789::Old::NORMAL
```


Otázky
???

NASLEDUJÚCE WEBINÁRE

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

KONTAKTUJTE NÁS

MAREK KONEČNÝ

CONSULTANT SENIOR

ZABBIX CERTIFIED TRAINER AND EXPERT

Mobil: +421 905 618 324

E-mail: marek.konecny@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