ZABBIX

ZABBIX – ZABBIX MONITORING

ČESKÝ ZABBIX ONLINE MEETUP

1 Úvod

ICZ

Skupina ICZ - základní údaje

- Systémový integrátor ICT řešení
- Společnost založena 1997
- Sídlo společnosti v Praze
- Působnost: ČR, SR, CEE, Asie, Afrika
- 550 zaměstnanců

S.ICZ - Dceřiná společnost

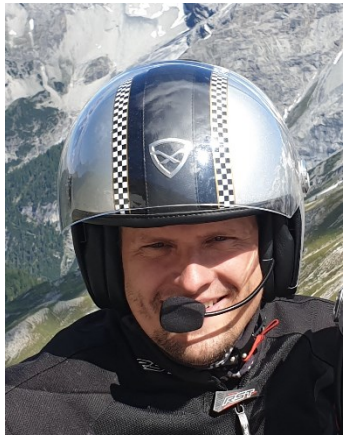
- Sekce Bezpečnost
- Řízení bezpečnosti informací (ISMS)
- Důvěryhodná výpočetní základna®
- IS k zpracování utajovaných informací
- Certifikované kryptografické prostředky
- ZABBIX - Primárně využíván pro dohled řešení zákazníků v rámci svěřené správy

S.ICZ

- ZABBIX Certified Partner od roku 2016

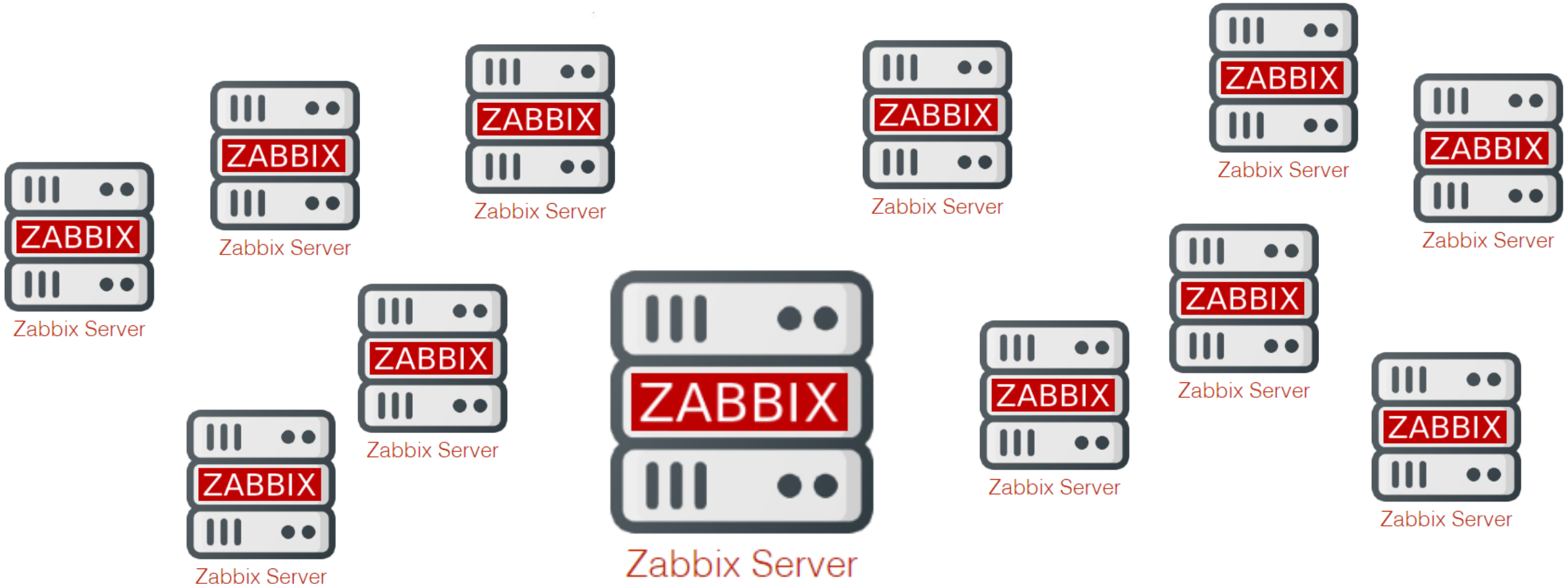
Alois Zadražil

- ZABBIXu se věnuji od roku 2010, od ZABBIX verze 1.8
- ZABBIX Certified Expert



Distribuovaný dohled

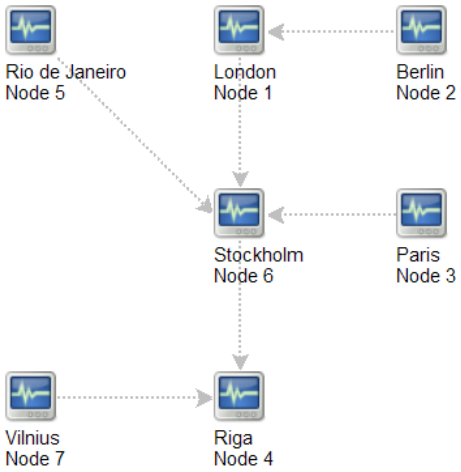
Cíl: Jedním ZABBIX serverem sledovat „podřízené“ ZABBIX servery, ale ne jen stav ZABBIX serveru, ale primárně vybrané události, které produkuje



Historie x Budoucnost?

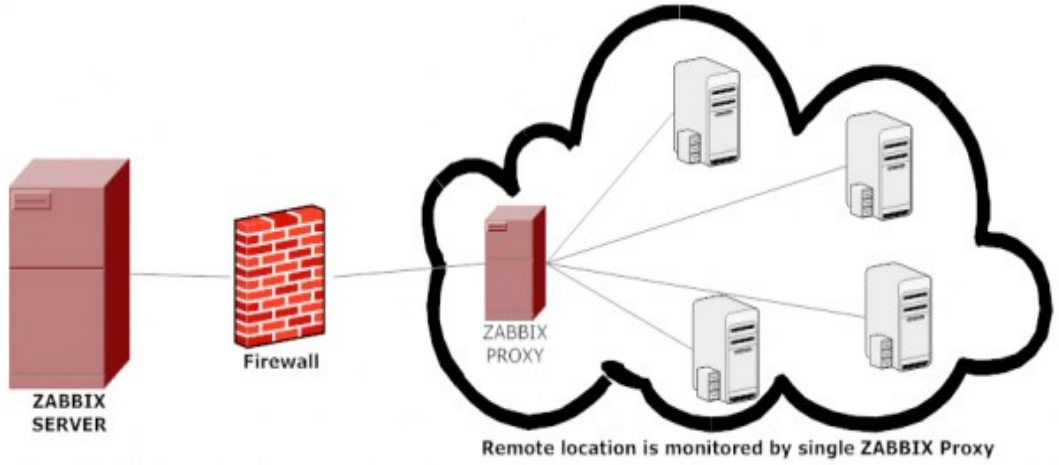
ZABBIX verze 2.2 Distribuovaný monitoring

- ✔ Skončil ve verzi 3.0
- ✔ Náhradou je pouze použití ZABBIX proxy



Distribuovaný dohled pomocí ZABBIX proxy

- ✔ Distribuce zátěže
- ✔ „Lokalitní“ sběr dat



2 Návrh řešení

Potřeby a cíl řešení

ZABBIX

Proč chtít informace z jiných ZABBIX serverů?

- ✔ Spravujete pro zákazníky ZABBIX servery a další zařízení – chcete mít centrální přehled
- ✔ Zákazníci mají vlastní ZABBIX servery a povolí vám přeposílání, ale ne jiné sledování svěřených služeb

Prvotní úvahy:

- ✔ Více zdrojů informací
- ✔ Synchronizace konfigurace
- ✔ Využití ZABBIX proxy
- ✔ Odesílání událostí

Využití prostředků nativních ZABBIX serverů – bez programování a psaní skriptů!!!

Základní koncept

Sledované ZABBIX servery odesílají události centrálnímu ZABBIX serveru

- ✔ Odeslání informace při vzniku problému
- ✔ Odeslání informace při Recovery

Filtr událostí – Akce

- ✔ Filtr podle potřeb na sledovaném ZABBIX serveru

Odesílání událostí

- ✔ Zabbix senderem
- ✔ Log soubor
- ✔ ZABBIX agentem
- ✔ Skriptem

Syntaxe události

- ✔ Vlastní syntaxe
- ✔ JSON, XML, ...

Datový formát - JSON

```
"{
"ZBX_event":"Error“,
"Host":"{HOST.NAME}",
"Event":"{EVENT.NAME}",
"Severity":"{EVENT.SEVERITY}",
"ID":"{EVENT.ID}",
"Time":"{EVENT.TIME}"
}"
```

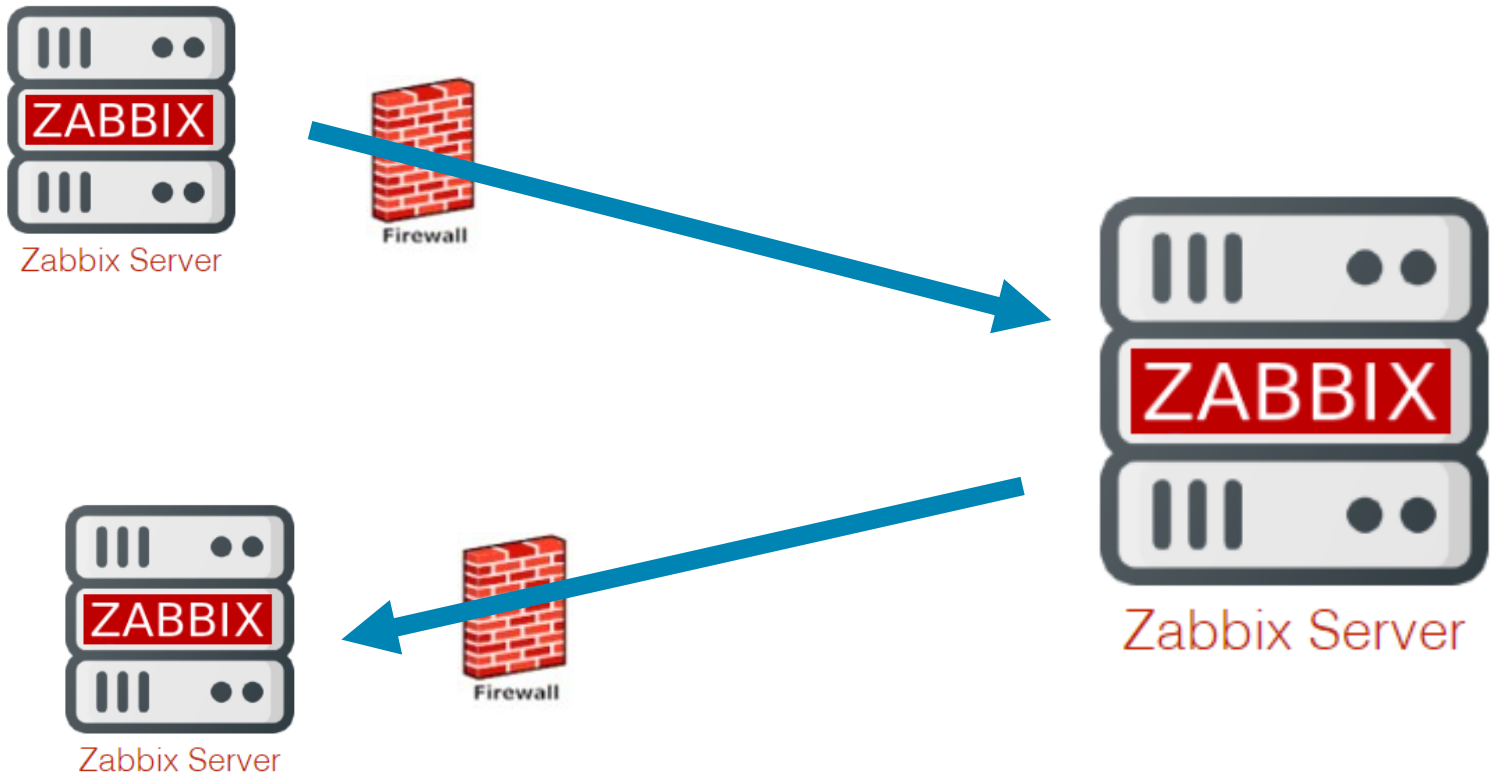
```
"{
"ZBX_event":„OK“,
"Host":"{HOST.NAME}",
"Event":"{EVENT.NAME}",
"Severity":"{EVENT.SEVERITY}",
"ID":"{EVENT.ID}",
"Time":"{EVENT.TIME}"
}"
```

Datový formát - XML

Formát použitý mým kolegou z ICZ sekce Infrastruktura:

<ZBX_event>Error</ZBX_event>
<Host>{HOST.NAME}</Host>
<Event>{EVENT.NAME}</Event>
<Severity>{EVENT.SEVERITY}</Severity>
<ID>{EVENT.ID}</ID>
<Time>{EVENT.TIME}</Time>

Active x Passive



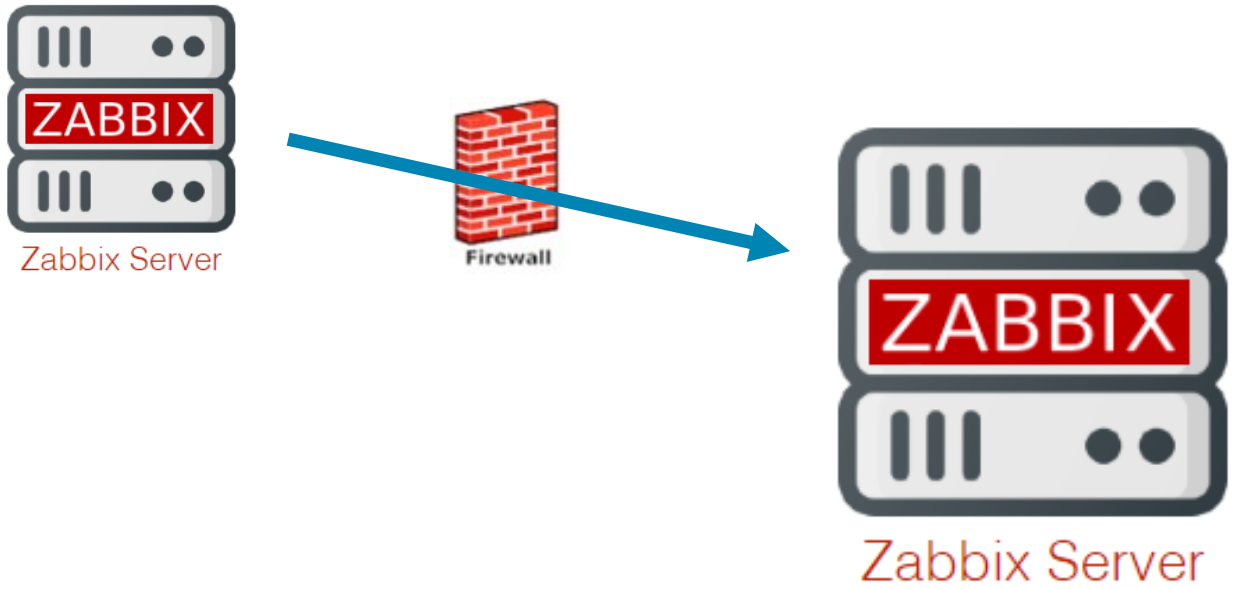
Active

Zabbix_sender

- Akce volá přímo Zabbix_sender s potřebnými daty

Active agent

- Akce ukládá data do log souboru
- Pomocí Active agenta a Itemu typu LOG posílá agent data serveru



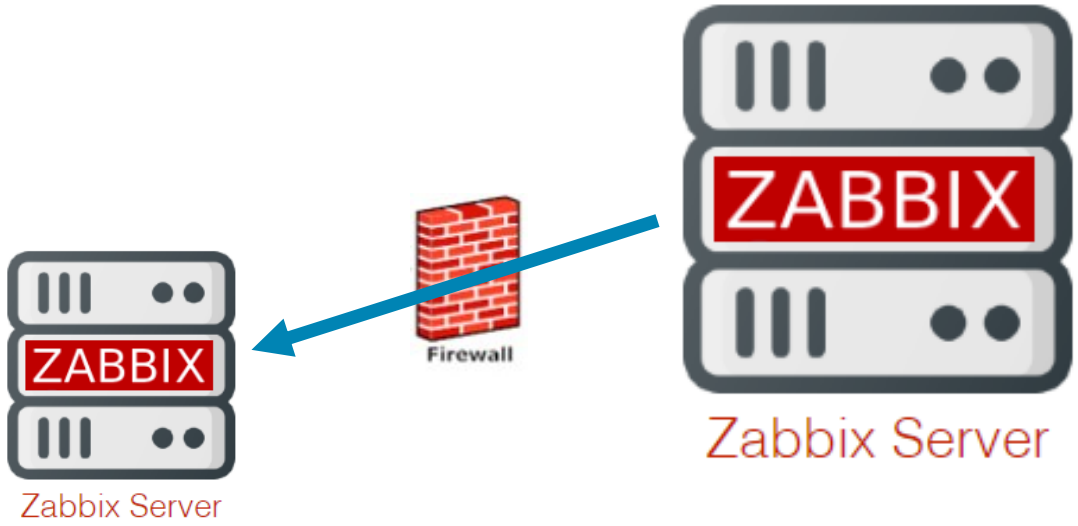
Passive

Passive

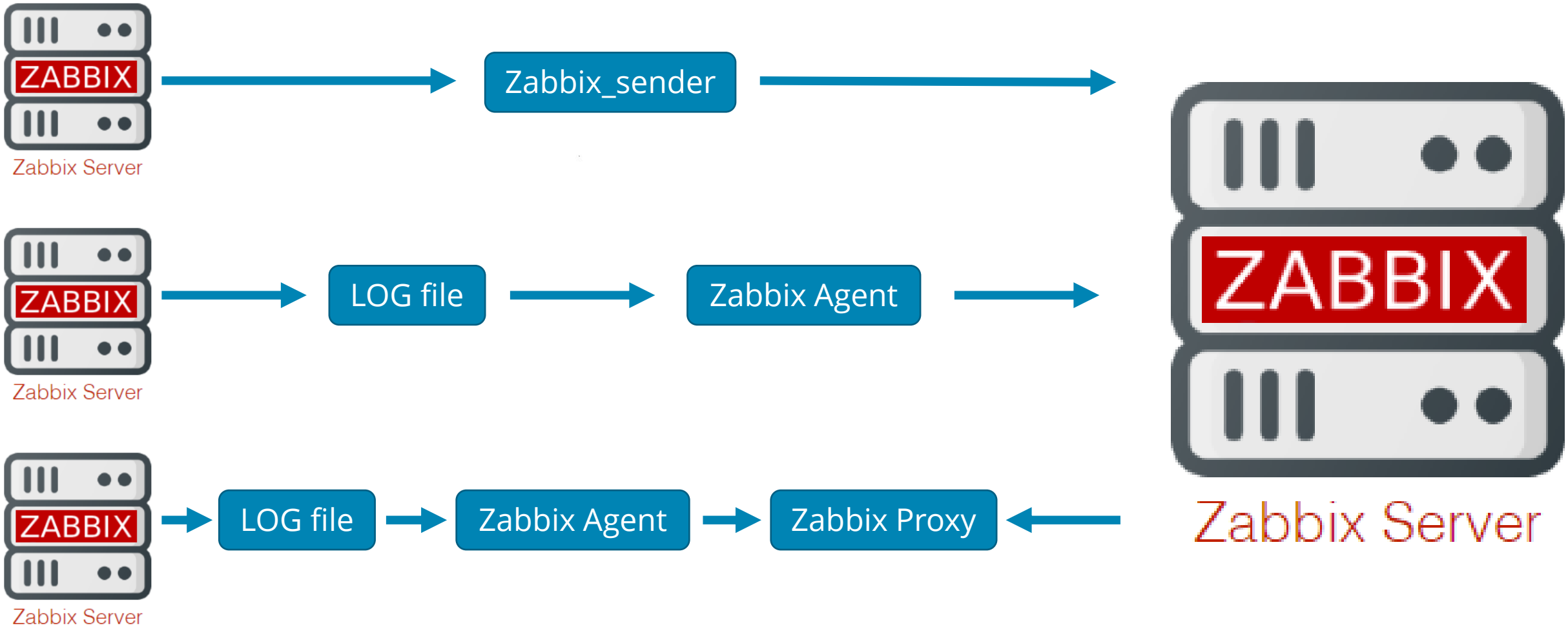
- ?? Problematické řešení
- Passive agent neumí Item typu LOG
- HTTP x SSH agent

Kombinace procesů a využití ZABBIX proxy

- Akce uloží data do LOG souboru
- aktivní agent čte LOG soubor a data předává lokální pasivní proxy



Varianty řešení



3 Praktická realizace

Odesilatel – Akce typu Remote command

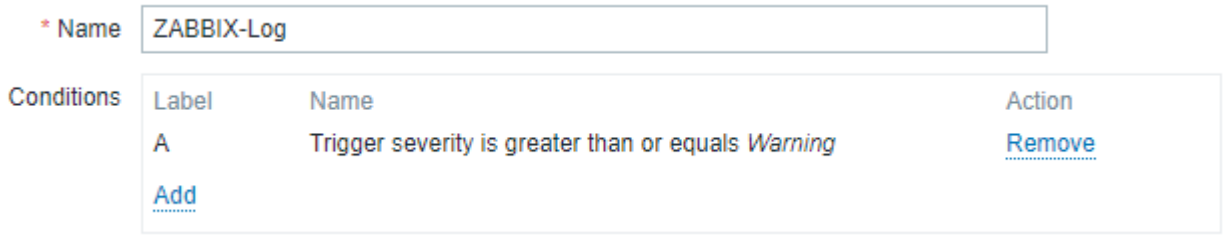
ZABBIX

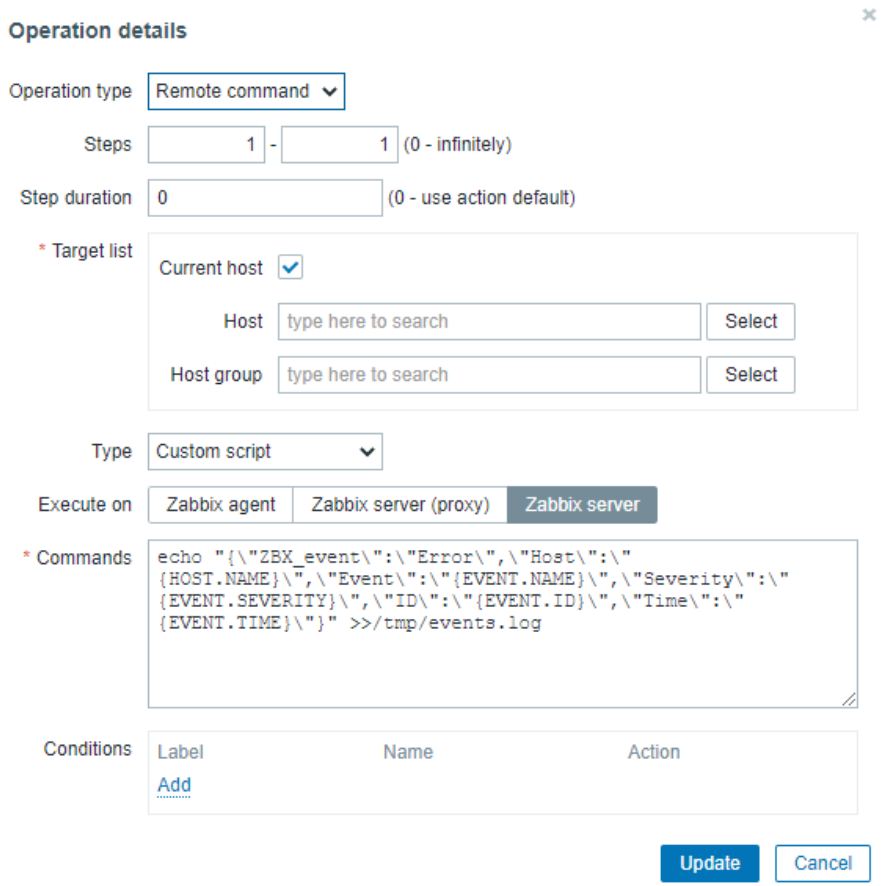
Condition:

- ✔ Trigger severity is greater than or equals Warning

Operation:

- ✔ echo "{\"ZBX_event\":\"Error\",\"Host\":\"{HOST.NAME}\",\"Event\":\"{EVENT.NAME}\",\"Severity\":\"{EVENT.SEVERITY}\",\"ID\":\"{EVENT.ID}\",\"Time\":\"{EVENT.TIME}\"}" >>/tmp/events.log

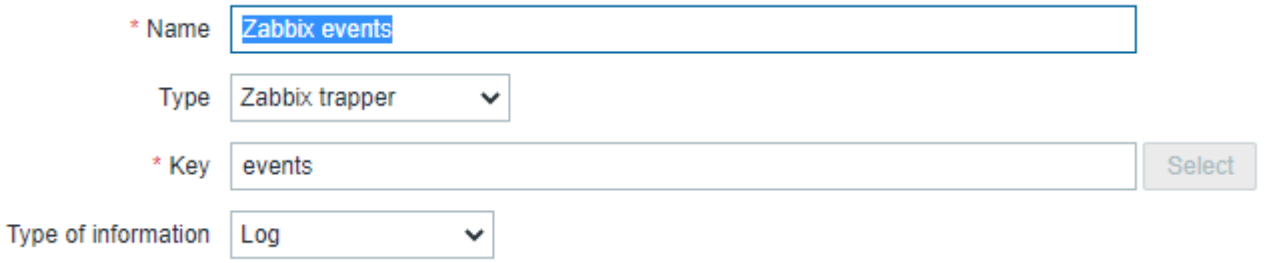




Příjemce – Item typu Log

Vytvoření jednoduchého Itemu

- ✔ Zabbix Trapper x Active Agent
- ✔ Log



Ukázka příchozích dat:

2020-10-09 08:46:43 {"ZBX_event":"Error","Host":"BACKUP","Event":"CPU utilization on BACKUP is over 80% for 15 min","Severity":"Warning","ID":"54894705","Time":"02:10:03"}

2020-10-09 08:46:43 {"ZBX_event":"OK","Host":"BACKUP","Event":"CPU utilization on BACKUP is over 80% for 15 min","Severity":"Warning","ID":"54894367","Time":"01:45:03"}

2020-10-09 08:46:43 {"ZBX_event":"Error","Host":"BACKUP","Event":"CPU utilization on BACKUP is over 80% for 15 min","Severity":"Warning","ID":"54894367","Time":"01:45:03"}

2020-10-09 08:46:43 {"ZBX_event":"Error","Host":"NBKASKOVA","Event":"ON","Severity":"Information","ID":"54892912","Time":"23:57:27"}

2020-10-09 08:46:43 {"ZBX_event":"OK","Host":"BACKUP","Event":"CPU utilization on BACKUP is over 80% for 15 min","Severity":"Warning","ID":"54892016","Time":"22:57:03"}

2020-10-09 08:46:43 {"ZBX_event":"Error","Host":"BACKUP","Event":"CPU utilization on BACKUP is over 80% for 15 min","Severity":"Warning","ID":"54892016","Time":"22:57:03"}

Triggers

ZABBIX

Name:

- ✔ Event on: {{ITEM.VALUE}.regsub("\"Host\":\"([^\"]*)\"", \1)}

Expression:

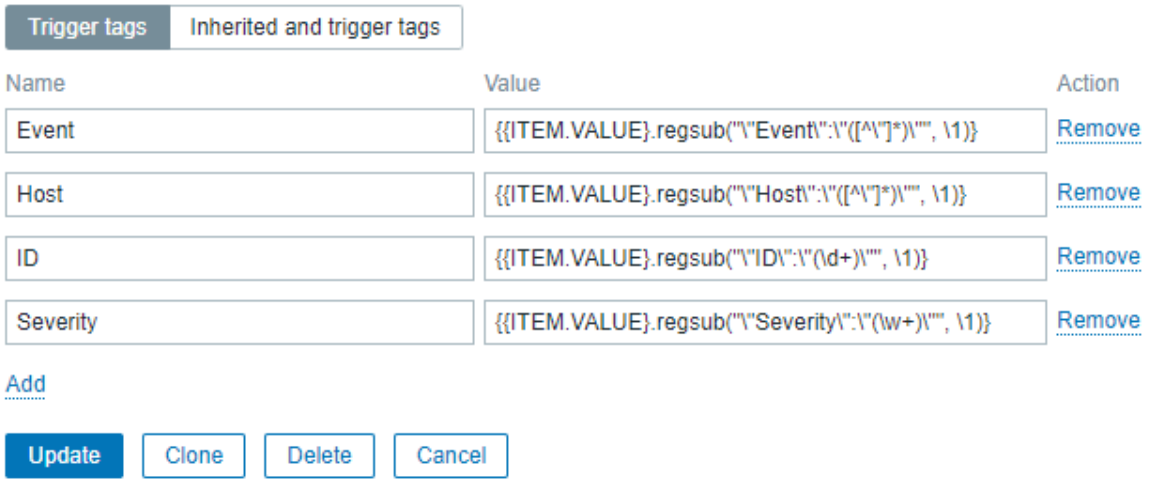
- ✔ {ZABBIX-ZABBIX_agent_v2:log[/tmp/events.log].regexp("\"ZBX_event\":\"Error\"")}=1
- ✔ and
- ✔ {ZABBIX-ZABBIX_agent_v2:log[/tmp/events.log].regexp("\"Severity\":\"Average\"")}=1

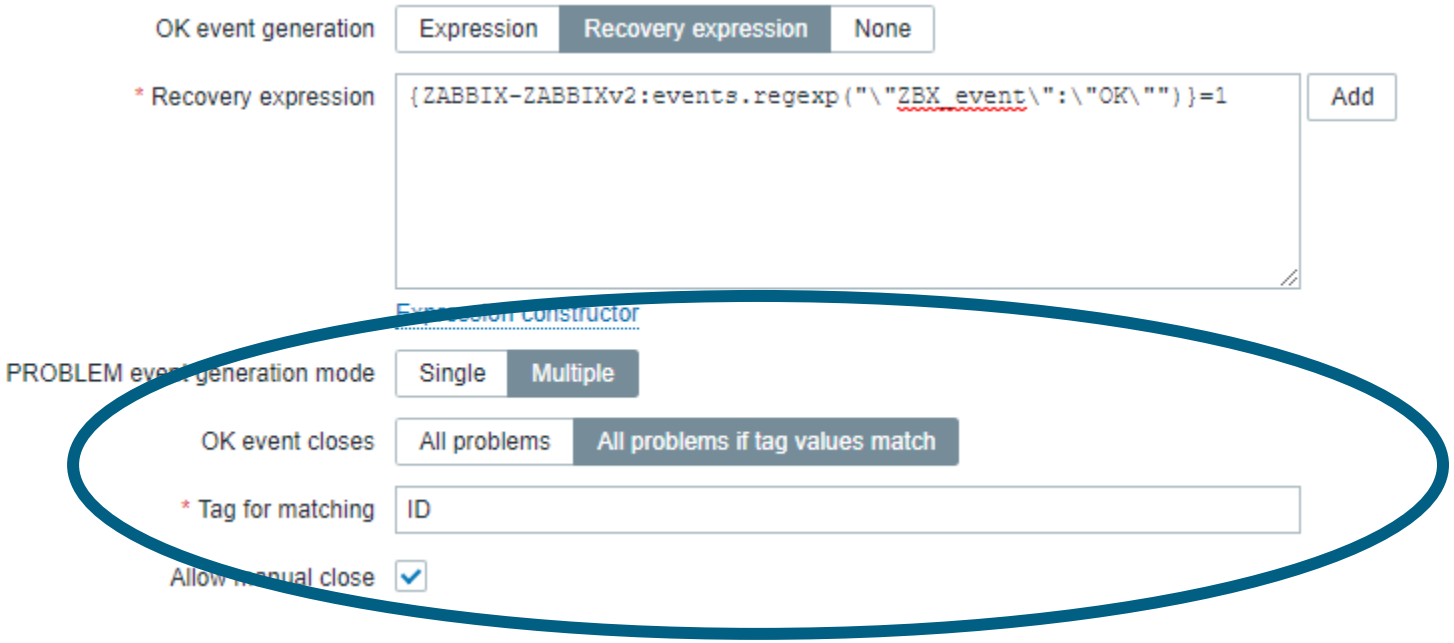
Recovery Expression:

- ✔ {ZABBIX-ZABBIX_agent_v2:log[/tmp/events.log].regexp("\"ZBX_event\":\"OK\"")}=1

Kouzlo Tagů

- Na každém ZABBIX serveru vznikne více událostí
- Jednoznačný identifikátor = Event ID
- Využití Tagů pro recovery





4 Ukázka

5 Závěrečná úvaha, bezpečnost a rozvoj

Spolehlivost, rozvoj

ZABBIX

Akce – Zabbix_sender

- ✔ Malá spolehlivost – při nedostupnosti serveru event. vypadne

Agent2 buffer

- ✔ Spolehlivost postavená na funkcionalitě active agenta

Heart-beat zprávy

- ✔ Ověřování komunikace a stavu

Použití jiných přenosových protokolů

- ✔ HTTP, SMTP ?

Bezpečnost

Šifrování, šifrování, šifrování....

TLS spojení mezi agentem a serverem

TLS pro ZABBIX sender

Reálné nasazení a limity

- Důležitá je syntaxe zpráv
- Obsahová disciplína – vynechání oddělovačů v textu Itemů, triggerů (v mém případě uvozovky)
- JSON x XML – formát závisí na sympatiích realizátora a zkušenosti s regulárními výrazy

! Děkuji za pozornost

ČESKÝ ZABBIX ONLINE MEEETUP

ČESKÝ

ZABBIX MEETUP ONLINE '20

Hlavní organizátor:

CoreIT

Spoluorganizátoři:

DATA SYS

ICZ

TOTALSERVICE

Q A OTÁZKY A ODPOVĚDI

- Všichni účastníci jsou ztlumeni, abychom eliminovali hluk
- Otázky prosím pište do sekce Q&A, ne do chatu
- Chat používejte pro diskuzi, networking nebo potlesk
- Pokud chcete vložit na sociální média nějaký příspěvek týkající se této akce, použijte hashtag: **#ZabbixMeetupOnline**

Kontakty

Telefon:	+420 222 271 111
Web:	https://www.iczgroup.com
Email:	alois.zadrazil@i.cz
LinkedIn:	https://www.linkedin.com/company/iczgroup/