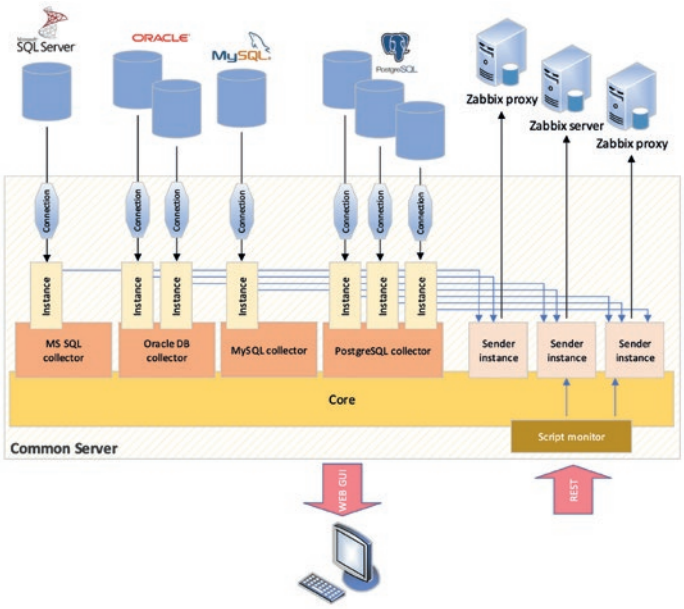
S&T – AUTOR ROZŠÍRENÍ A MODULOV PRE MONITOROVACÍ NÁSTROJ ZABBIX

S&T je autorom a dodávateľom viacerých doplnkov pre monitorovací nástroj Zabbix. Naše rozšírenia a moduly sú vyvíjané pre heterogénne prostredia a podporujú širokú množinu operačných platforiem (Linux, HPUX, Solaris, AIX, MS Windows). Využívané sú nové funkcionality produktu Zabbix ako napr. globálna korelácia alebo obohacovanie generovaných incidentov (Zabbix event tags). Ponúkaná implementáciu rozšírení a modulov pozostáva z piatich skupín:

- Monitoring heterogénneho prostredia databáz (Oracle, MS SQL, PostgreSQL, MySQL, MariaDB, Galera) – modul **Common Server**
- Monitoring log súborov a SNMP trapov – modul **TBC** (Time Based Correlation)
- Monitoring rozsiahlych heterogénnych prostredí serverov na úrovni OS – modul **Prefabrikáty**
- Centrálny repozitár konfigurácií monitorovaných serverov, distribúcia konfigurácia a vzdialená správa Zabbix agenta a Zabbix proxy – rozšírenie **Distribučný systém**
- Časované automatické uzatváranie incidentov

Všetky rozšírenia a moduly sú dodávané v podobe skriptov s otvoreným kódom, konfiguračných súborov a Zabbix šablón bez licenčných obmedzení. Zákazník môže dodané riešenie ľubovoľne upravovať a využívať. Súčasťou dodávky je podrobná inštalačná aj administračná dokumentácia.

Moduly a rozšírenia môžu byť upravené podľa špecifických potrieb zákazníka a v prípade požiadavky zo strany zákazníka sú k nim poskytované aj školenia.



Architektúra modulu Common Server

MONITORING PROSTREDIA DATABÁZ – MODUL COMMON SERVER

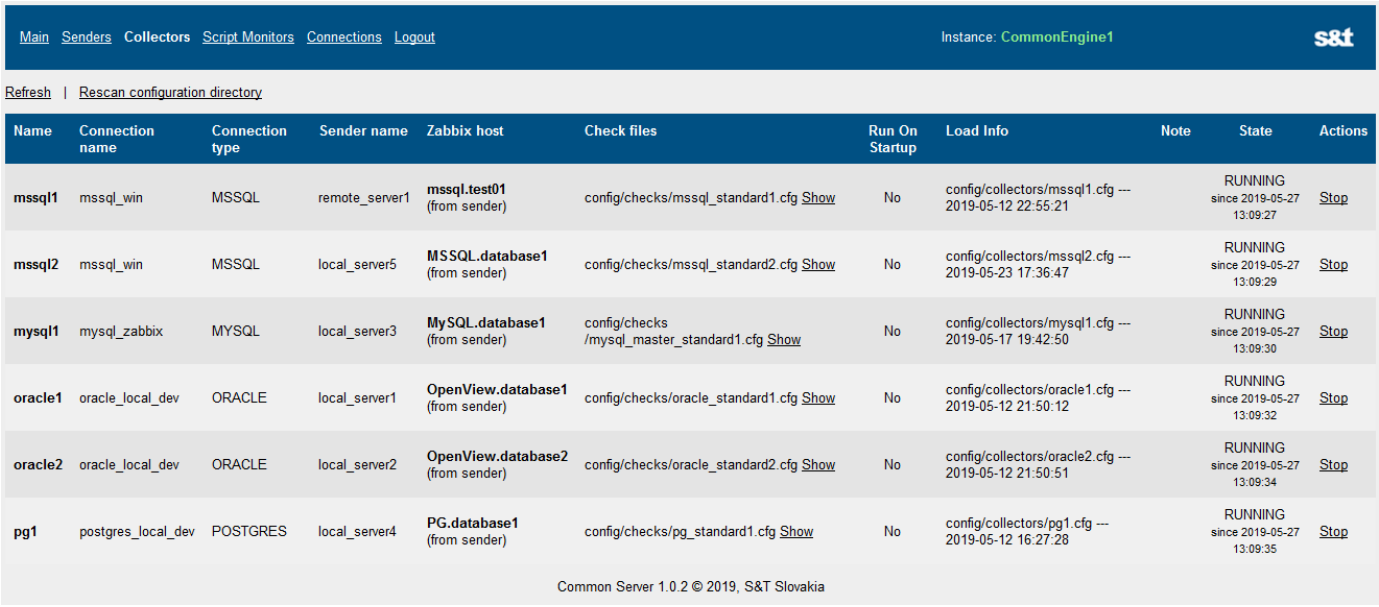
Modul Common Server poskytuje možnosť realizácie fault a performance monitoringu heterogénneho prostredia databáz (Oracle, MS SQL, PostgreSQL, MySQL, MariaDB, Galera) s nasledovnou funkcionalitou a vlastnosťami:

- Agent less monitoring – modul nevyužíva Zabbix agentov, ale odovzdáva údaje prostredníctvom Zabbix sender nástroja zozbierané pomocou vlastných kolektorov vytvorených pre jednotlivé typy databáz s možnosťou šifrovania komunikácie
- Jednoduchá a unifikovaná konfigurácia zberu údajov z databáz – monitoring každej inštancie databázy pomocou jej kolektora je popísaný samostatným alebo zdieľaným konfiguračným súborom alebo súbormi ponúkajúcimi nasledovné nastavenia:
  - Autodiscovery metrík z údajov v databáze
  - Časovanie zberu údajov na základe definovania intervalov
  - Prahové hodnoty definované pre metriky uvedené priamo v konfiguračnom súbore alebo pomocou hodnôt v databáze
  - Nastavenie obohacovania generovaných problémov pomocou statických údajov uvedených priamo v konfiguračnom súbore alebo pomocou hodnôt v databáze
- Self monitoring:
  - sledovanie úspešnosti a doby získavania jednotlivých monitorovaných hodnôt
  - sledovanie aktivity jednotlivých inštancií Common Servera a jeho kolektorov (RAM, CPU)
- Tabuľky udalostí – zbieranie a nasledovná korelácia udalostí prezentovaných obsahom konkrétnej tabuľky alebo tabuliek (funkcionalita zabezpečuje fungovanie integrácií Zabbixu so špecifickými zdrojmi udalostí, ktoré majú podobu záznamov vo vybraných tabuľkách databázy)
- Script monitor – spúšťanie ľubovoľných skriptov prostredníctvom REST rozhrania, ktorých výstup je odovzdávaný do Zabbixu spolu s monitorovaním doby trvania a úspešnosti ich zbiehania
- Web GUI – každá inštancia Common Servera disponuje vlastným web rozhraním, pomocou ktorého je možné spravovať všetky jej bežiace komponenty a prezerať nasadenú konfiguráciu
- Collector health – dashboard prezentujúci stav inštancie konkrétneho kolektora (RAM, CPU, doby trvania zberu údajov, verzia databázy a kolektora)
- Jednoduchá inštalácia – Common Server tvorí skupina skriptov napísaná v jazyku Python. Podmienkou behu je prítomnosť Python interpretera a skupiny Python modulov.

V monitorovanom prostredí môže bežať ľubovoľný počet inštancií Common Servera a každá môže pomocou ľubovoľného počtu inštancií kolektorov aktívne monitorovať viacero odlišných typov databáz a odosielať údaje do rozličných cieľových Zabbix proxy alebo Zabbix serverov.

S&T Slovakia s.r.o. | Mlynské nivy 71 | 821 05 Bratislava | Tel.: +421 258 273 111 | E-mail: snt@snt.sk | www.snt.sk

ZABBIX PREMIUM PARTNER

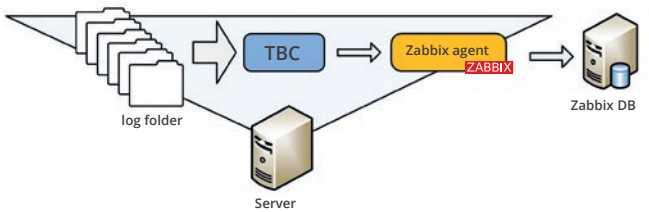


Web GUI modulu Common Server – prezentácia aktivity kolektorov

MONITORING LOG SÚBOROV A SNMP TRAPOV – MODUL TBC

Modul TBC (Time Based Correlation) poskytuje podrobný monitoring veľkého objemu log súborov a SNMP trapov. Modul umožňuje:

- Monitoring pomocou Zabbix agenta (log súbory) a Zabbix proxy (SNMP trapy) – nie je potrebné inštalovať žiadne ďalšie aplikácie alebo databázy, modul tvorí jeden skript a jeho konfiguračné súbory definujúce tzv. korelátory
- Monitoring samostatných log súborov a alebo celých adresárov – stačí zadefinovať adresár a monitorovaný je jeho celý jeho obsah vrátane podadresárov alebo jeho časť (log súbory môžu v adresároch voľne vznikať aj zanikať)
- Monitoring log súborov s viacriadkovým typom záznamov (multiline logs)



Architektúra implementácie modulu TBC pre monitoring adresárov s log súbormi

- Možnosť konfigurácie ľubovoľných korelačných a filtračných pravidiel už na úrovni Zabbix agenta alebo Zabbix proxy – do databázy Zabbixu tečú len korelované a filtrované záznamy, ktoré majú byť podkladom pre vznik incidentov. Súčasťou dodávky je viacero najčastejšie používaných pravidiel v podobe korelátorov:
  - Suppresing – potláčanie alebo prepúšťanie vybraných typov záznamov/trapov
  - Repeating – prepustenie záznamu/trapu v prípade naplnenia definovaného počtu jeho opakovaní
  - Time suppresing – potláčanie vybraných typov záznamov/trapov definovaný čas
  - Inhibition – prepustenie záznamu/trapu ak do stanoveného času neobjaví iný zadefinovaný typ záznamu/trapu
- Počítanie duplikátov – všetky korelátory zároveň počítajú aj počet výskytov určitého typu záznamu/trapu za účelom prezentácie počtu duplikátov jednotlivých typov incidentov v prostredí Zabbixu.
- Self monitoring – sledovanie behu modulu TBC na jednotlivých Zabbix agentoch a Zabbix proxy

MONITORING SERVEROV NA ÚROVNI OS – MODUL PREFABRIKÁTY

Modul zjednodušuje a urýchľuje nasadenie monitoringu a jeho administráciu na úrovni OS pre veľké počty serverov v heterogénnych prostrediach aj v konfiguráciách active/passive a active/active klastrov. Modul umožňuje realizovať konfiguráciu monitoringu procesov, služieb, sieťových socketov, spojení a zaplnenia súborových systémov len pomocou jednoduchých konfiguračných súborov určených pre konkrétny server, bez nutnosti zasahovať do grafického rozhrania Zabbixu alebo reštartovať ktorýkoľvek jeho komponent. Modul zabezpečuje monitoring:

- behu procesov a služieb – konfigurácia monitoringu behu procesov a služieb; monitoruje sa beh procesu alebo služby, účet, pod ktorým beží a počet inštancií
- stavu socketov a spojení pre TCP/UDP protokoly – monitoruje sa aktivita socketov a v prípade TCP aj celých spojení (stavy LISTEN, ESTABLISHED...)
- obsadenia lokálnych aj sieťových súborových systémov – monitoruje sa voľné miesto súborových systémov v percentách aj v megabajtoch; prahové hodnoty sú uvádzané pre dve úrovne závažnosti priamo v konfiguračných súboroch; monitorovaný je aj stav súborového systému (odpojený/pripojený)

Modul poskytuje monitoring výkonnostných metrík (napr. CPU, RAM, SWAP), ktorých množinu je možné ľubovoľne dopĺňať. Konfigurácia prahových hodnôt je vytváraná pomocou Zabbix makier.

V konfiguračných súboroch je možné pre monitorované komponenty uviesť napr. názov služby, závažnosť otváraného incidentu, príp. vytvoriť ďalšie atribúty, o ktoré budú otvorené incidenty v prostredí Zabbixu obohatené v podobe tzv. Zabbix event tags.

Príklad obrazovky (Zabbix screen) generovanej modulom Prefabrikáty

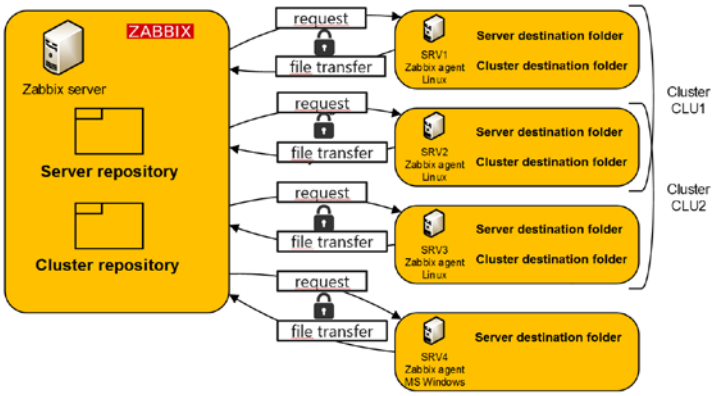
CENTRÁLNY REPOZITÁR KONFIGURÁCIÍ – ROZŠÍRENIE DISTRIBUČNÝ SYSTÉM

Rozšírenie dopĺňa funkcionalitu Zabbixu o **možnosť vytvorenia centrálneho repozitára alebo repozitárov konfigurácii agentov monitorovaných serverov za účelom jeho distribúcie na jednotlivé servery alebo celé klastre v heterogénnom prostredí.** Distribučný systém umožňuje distribuovať monitorovacie skripty alebo binárne súbory rozširujúce funkcionalitu Zabbix agenta, konfiguračné súbory monitorovacích skriptov alebo konfiguračné súbory Zabbix agentov. Rozšírenie ďalej umožňuje vzdialenú správu Zabbix agentov a Zabbix proxy. Tvorcovia dohľadu tak nepotrebujú priamo pristupovať na monitorované servery v procese konfigurácie monitoringu a jeho zmien. Vzdialene je možné vykonávať nasledovné úkony nad všetkými monitorovanými servermi:

- vykonanie príkazu na monitorovanom serveri
- výpis konfiguračných súborov agenta na monitorovanom serveri
- distribúcia obsahu repozitára na monitorovaný server alebo klaster
- výpis aktuálneho obsahu distribučného adresára na monitorovanom serveri
- zistenie stavu, zastavenie a reštart Zabbix agenta na monitorovanom serveri
- zistenie stavu, update, zastavenie a štart Zabbix proxy

Na monitorovaných serveroch nie je nutné inštalovať žiadneho ďalšieho agenta, vytvárať nové účty ani otvárať ďalšie porty na firewalle, využívaný je Zabbix agent a komunikácia je prostredníctvom neho zabezpečená šifrovaním.

Rozšírenie je otvorené a je ho možné dopĺňať o nové funkcionality a nástroje. Napr. v prípade využívania modulu Prefabrikáty alebo TBC, sú súčasťou dodávky Distribučného systému aj nástroje pre vzdialenú správu týchto modulov.



Príklad implementácie rozšírenia Distribučný systém

ČASOVANÉ AUTOMATICKÉ UZATVÁRANIE INCIDENTOV

Modul umožňuje nastaviť na úrovni Zabbix triggera dobu platnosti ním otváraného incidentu. Po uplynutí nastaveného času, sa incident automaticky uzatvorí. Platnosť je možné definovať v hodinách alebo dňoch. **Toto riešenie zabezpečí automatické uzatváranie incidentov aj v prípade, že pre daný typ incidentu neexistuje automatická opravná podmienka alebo akcia.**

Konfigurácia automatického časovaného uzatvárania doplňuje ostatné techniky uzatvárania incidentov, ktoré s ňou môžu koexistovať – to znamená, že konkrétny incident môže byť uzatvorený viacerými situáciami/stavmi, záleží na tom, ktorá situácia/stav nastane skôr:

- Príčina incidentu zanikla
- Deduplikácia incidentu
- Incident bol manuálne uzatvorený operátorom
- Incident bol uzatvorený po nastavenej dobe platnosti