

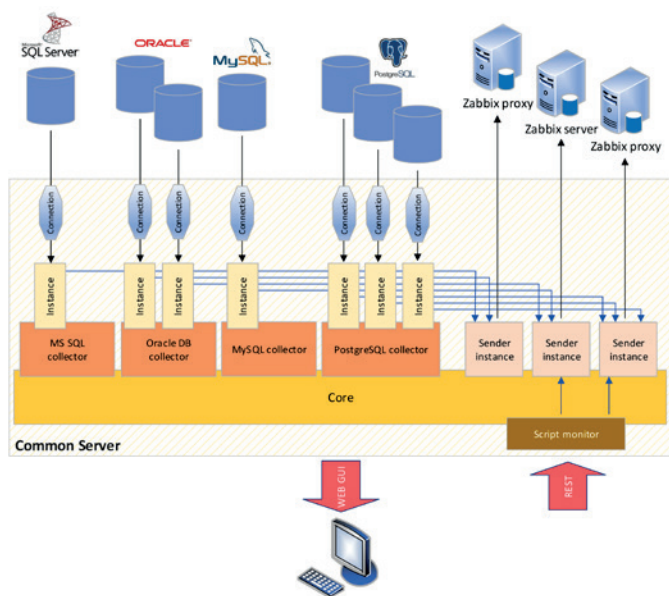
Axians Slovakia – autor rozšírení a modulov pre monitorovací nástroj Zabbix

Axians Slovakia 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 implementácia rozšírení a modulov pozostáva z piatich skupín:

- ▶ Monitoring heterogénneho prostredia databáz (Oracle, MS SQL, PostgreSQL, MySQL, MariaDB, Galera) – modul **Common Server**
- ▶ Tvorba stromu služieb – modul **BSM** (Business Service Management)
- ▶ Monitoring SAP ERP prostredia prostredníctvom CCMS – modul **SAP**
- ▶ 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 inštalácia 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:
 1. Autodiscovery metrick z údajov v databáze
 2. Časovanie zberu údajov na základe definovania intervalov
 3. Prahové hodnoty definované pre metriky uvedené priamo v konfiguračnom súbore alebo pomocou hodnôt v databáze
 4. Nastavenie obohacovania generovaných problémov pomocou statických údajov uvedených priamo v konfiguračnom súbore alebo pomocou hodnôt v databáze
- ▶ **Self monitoring:**
 1. sledovanie úspešnosti a doby získavania jednotlivých monitorovaných hodnôt
 2. sledovanie aktivity jednotlivých inštancií Common Servera a jeho kolektorov (RAM, CPU)
- ▶ **Tabuľky udalostí** – zbieranie a nasledovná korelácia udalostí prezentovaných obsahom konkrétnej tabuľky alebo tabuliek (funkcionality 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 bežiacie komponenty a preerať 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.

Name	Connection name	Connection type	Sender name	Zabbix host	Check files	Run On Startup	Load Info	Note	State	Actions
mssql1	mssql_win	MSSQL	remote_server1	mssql.test01 (from sender)	config/checks/mssql_standard1.cfg Show	No	config/collectors/mssql1.cfg --- 2019-05-12 22:55:21		RUNNING since 2019-05-27 13:09:27	Stop
mssql2	mssql_win	MSSQL	local_server5	MSSQL.database1 (from sender)	config/checks/mssql_standard2.cfg Show	No	config/collectors/mssql2.cfg --- 2019-05-23 17:36:47		RUNNING since 2019-05-27 13:09:29	Stop
mysql1	mysql_zabbix	MYSQL	local_server3	MySQL.database1 (from sender)	config/checks/mysql_master_standard1.cfg Show	No	config/collectors/mysql1.cfg --- 2019-05-17 19:42:50		RUNNING since 2019-05-27 13:09:30	Stop
oracle1	oracle_local_dev	ORACLE	local_server1	OpenView.database1 (from sender)	config/checks/oracle_standard1.cfg Show	No	config/collectors/oracle1.cfg --- 2019-05-12 21:50:12		RUNNING since 2019-05-27 13:09:32	Stop
oracle2	oracle_local_dev	ORACLE	local_server2	OpenView.database2 (from sender)	config/checks/oracle_standard2.cfg Show	No	config/collectors/oracle2.cfg --- 2019-05-12 21:50:51		RUNNING since 2019-05-27 13:09:34	Stop
pg1	postgres_local_dev	POSTGRES	local_server4	PG.database1 (from sender)	config/checks/pg_standard1.cfg Show	No	config/collectors/pg1.cfg --- 2019-05-12 16:27:28		RUNNING since 2019-05-27 13:09:35	Stop

Common Server 1.0.2 © 2019, S&T Slovakia

Web GUI modulu Common Server – prezentácia aktivity kolektorov

TVORBA STROMU SLUŽIEB – MODUL BSM (BUSINESS SERVICE MANAGEMENT)

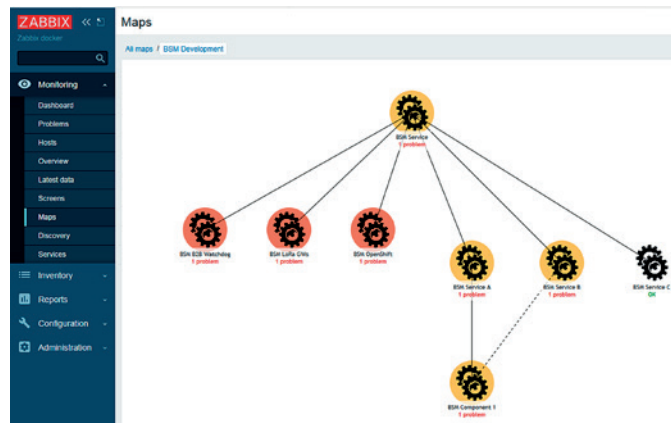
Modul BSM predstavuje unikátne riešenie modelovania a prezentácie stavu služieb prostredníctvom stromu služieb z množstvom dôležitých funkcionalít, ktoré posúvajú Zabbix na úroveň komerčných monitorovacích nástrojov:

- ▶ Grafická prezentácia stromu služieb
- ▶ **Výpočet stavu služieb (uzlov stromu služieb) na základe propagácie stavov medzi uzlami stromu a väzbou na udalosti pomocou tagov!**
- ▶ Väzba uzlov stromu na:
 1. Všetky problémy
 2. Nepotvrdené problémy (acknowledge)
 3. Nepotlačené problémy (suppressed – plánované výpadky)
- ▶ Notifikácie z uzlov stromu služieb pri zmene ich stavu
- ▶ SLA evaluácia na základe severity služby
- ▶ Root Cause Analysis (RCA)

Implementácia modulu je jednoduchá, nie sú vyžadované žiadne nástroje tretích strán, databázy, konfiguračné súbory. Celá konfigurácia je súčasťou konfigurácie Zabbixu a pre účely zálohovania postačuje zrealizovať zálohovanie databázy Zabbixu.

Benefity modulu BSM:

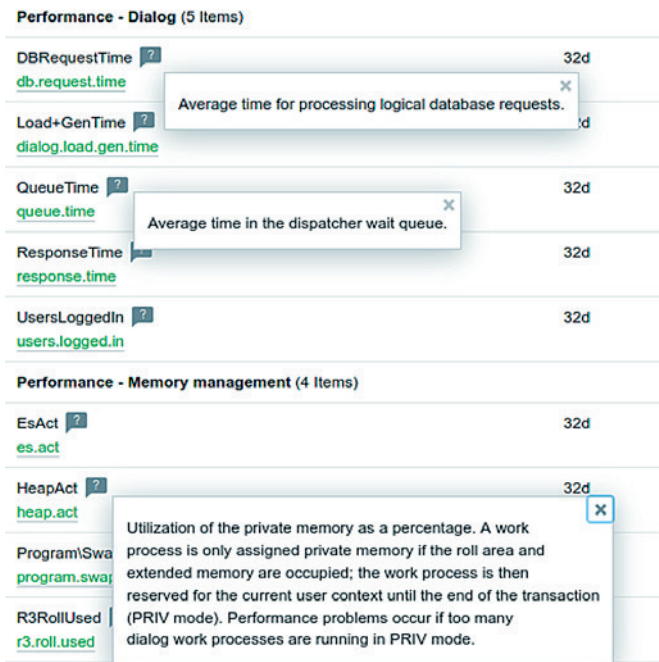
1. Okamžitý prehľad o stave služieb poskytovaných IT prostredím spoločnosti
2. Možnosť prezentovať impakt výpadkov na business procesy
3. Priama notifikácia (SMS, mail...) len v prípade zmeny stavu konkrétnych služieb v kompetencii konkrétneho manažéra
4. Okamžité informovanie o stave plnenia SLA za ľubovoľné obdobie (deň, týždeň, mesiac, rok)
5. RCA – identifikácia udalostí, ktoré nesú zodpovednosť za malígny stav danej služby a následne prístup ku konkrétnym metrikám pre účely nájdenia príčiny



Grafická prezentácia časti stromu služieb v grafickom rozhraní

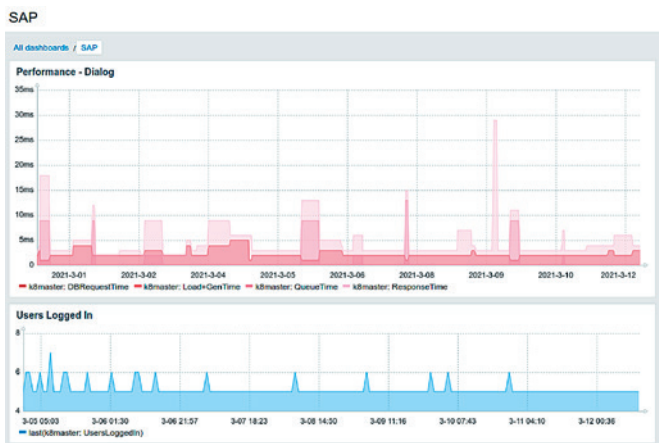
MONITORING SAP ERP PROSTREDIA PROSTREDNÍCTVOM CCMS – MODUL SAP

Pomocou integrácie na CCMS (Computing Center Management System) umožňuje Zabbix zber a vyhodnocovanie metriek z jednotlivých inštancií SAP systémov. Týmto spôsobom je zabezpečený centrálny tzv. „umbrella“ pohľad na firemnú IT infraštruktúru na jednom mieste v nástroji Zabbix. CCMS strom poskytuje množstvo metriek (stovky) nielen o stave konkrétnej SAP inštancie, ale aj o jej výkonnosti resp. performance metriek.



Príklady výkonnostných metriek

Predpokladom na zber dát je SAP užívateľ s heslom a rolou, ktorá umožní prístup k CCMS údajom. Integrácia môže byť nainštalovaná priamo na systéme spolu so Zabbix agentom alebo je možná jej inštalácia na Zabbix proxy (vzdialený zber dát). Riešenie je postavené a dodávané s otvoreným kódom spolu s návodom, ktorý umožňuje vytváranie špecifických metriek podľa potrieb zákazníka a ich vizualizáciu prostredníctvom dashboardov.



Ukážka dashboardu pre SAP modul

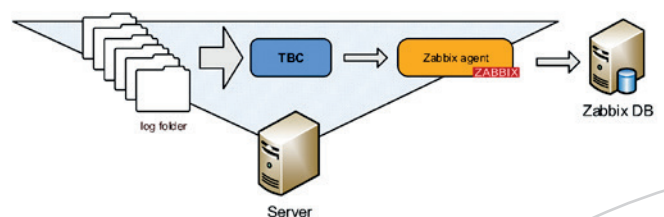
MONITORING LOG SÚBOROV A SNMP TRAPOV – MODUL TBC

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

- ▶ Monitoring pomocou Zabbix agenta (log súboru) a Zabbix proxy (SNMP trapu) – **nie je potrebné inštalovať žiadne ďalšie aplikácie alebo databázy**, modul tvorí jeden skript a jeho konfiguračné súbory definujúce tzv. korelátoru
- ▶ **Monitoring samostatných log súborov a alebo celých adresárov** – stačí zadať adresár a monitorovaný je jeho celý obsah vrátane podadresárov alebo jeho časť (log súbory môžu v adresároch voľne vznikáť aj zanikať)
- ▶ **Monitoring log súborov s viacriadkovým typom záznamov** (multiline logs)
- ▶ **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:
 1. **Suppresing** – potlačanie alebo prepúšťanie vybraných typov záznamov/trapov
 2. **Repeating** – prepustenie záznamu/trapu v prípade naplnenia definovaného počtu jeho opakovaní
 3. **Time suppresing** – potlačanie vybraných typov záznamov/trapov definovaný čas
 4. **Inhibition** – prepustenie záznamu/trapu ak do stanoveného času neobjaví iný zadaný typ záznamu/trapu
 5. **Storm detection** – detegovanie zvýšenej intenzity toku SNMP trapov z konkrétneho zdroja, blokovanie toku a jeho obnovenie po poklese nadmernej intenzity toku trapov

▶ **Počítanie duplikátov** – všetky korelátoru 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



Architektúra implementácie modulu TBC pre monitoring adresárov s log súborami

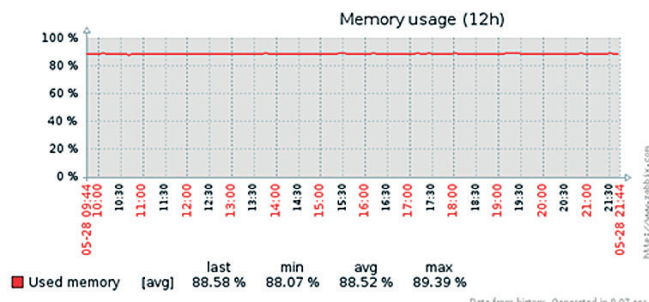
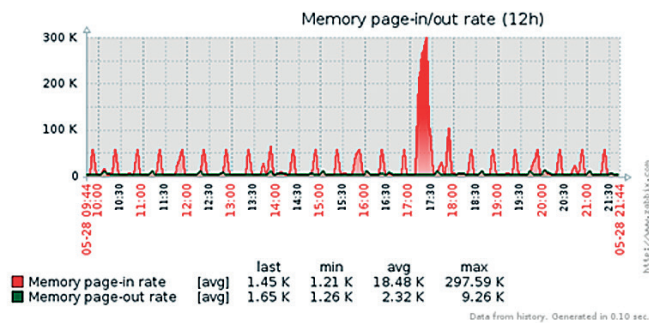
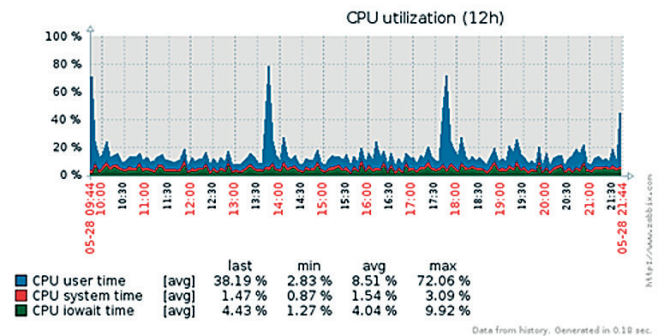
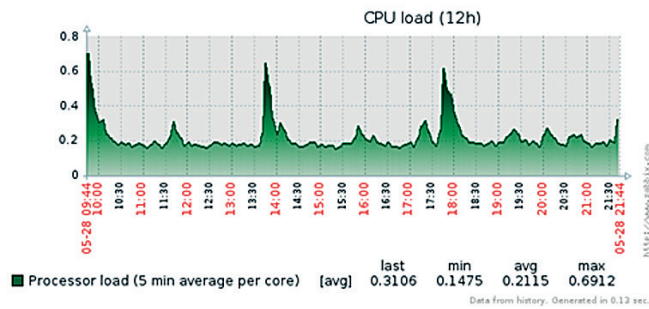
MONITORING SERVEROV NA ÚROVNI OS – MODUL PREFABRIKÁTY

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...)

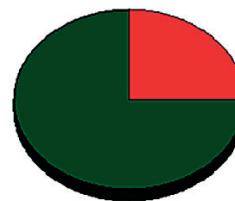
- ▶ **obsadenia lokálnych aj sieťových súborových systémov** – monitoruje sa voľné miesto súborových systémov v percentách aj v megabajtoch; prahové hodnoty sú uvádzané pre dve úrovne závažnosti priamo v konfiguračných súboroch; monitorovaný je aj stav súborového systému (odpojený/pripojený) Modul poskytuje monitoring výkonnostných metrick (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.



Swap usage (12h)

- Value: 4 GB (100%)
- Value: 1.01 GB (25.20%)



Total swap space [last]
Used swap space [last]

Data from history. Generated in 0.09 sec.

Príklad obrazovky (Zabbix screen) generovanej modulom Prefabrikáty

CENTRÁLNY REPOZITÁR KONFIGURÁCIÍ – ROZŠÍRENIE DISTRIBUČNÝ SYSTÉM

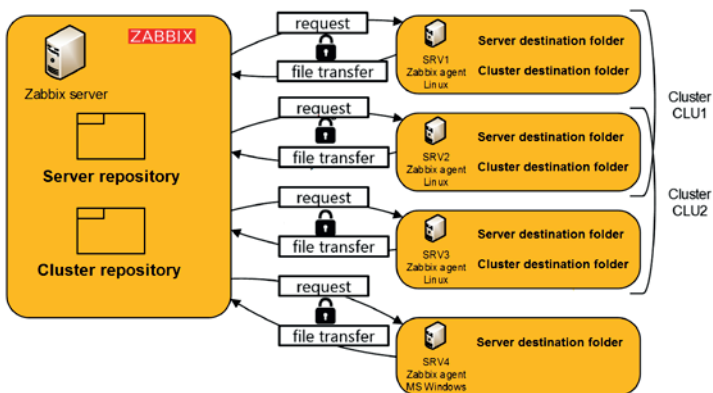
Rozšírenie dopĺňa funkcionality Zabbixu o **možnosť vytvorenia centrálného repozitára alebo repozitárov konfigurácií agentov monitorovaných serverov za účelom jeho distribúcie na jednotlivé servery alebo celé klastre v heterogénnom prostredí**. Distribučný systém umožňuje distribuovať monitorovacie skripty alebo binárne súbory rozširujúce funkcionality Zabbix agenta alebo Zabbix agent2, 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 klastre
- ▶ 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

Všetky uvedené úkony je možné vykonávať z grafického rozhrania Zabbixu alebo pomocou CLI nástrojov, ktoré je možné využívať pri tvorbe vlastných skriptov.

Na monitorovaných serveroch nie je nutné inštalovať žiadneho ďalšieho agenta, vytvárať nové účty ani otvárať ďalšie porty na firewall, využívaný je Zabbix agent alebo Zabbix agent2 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.



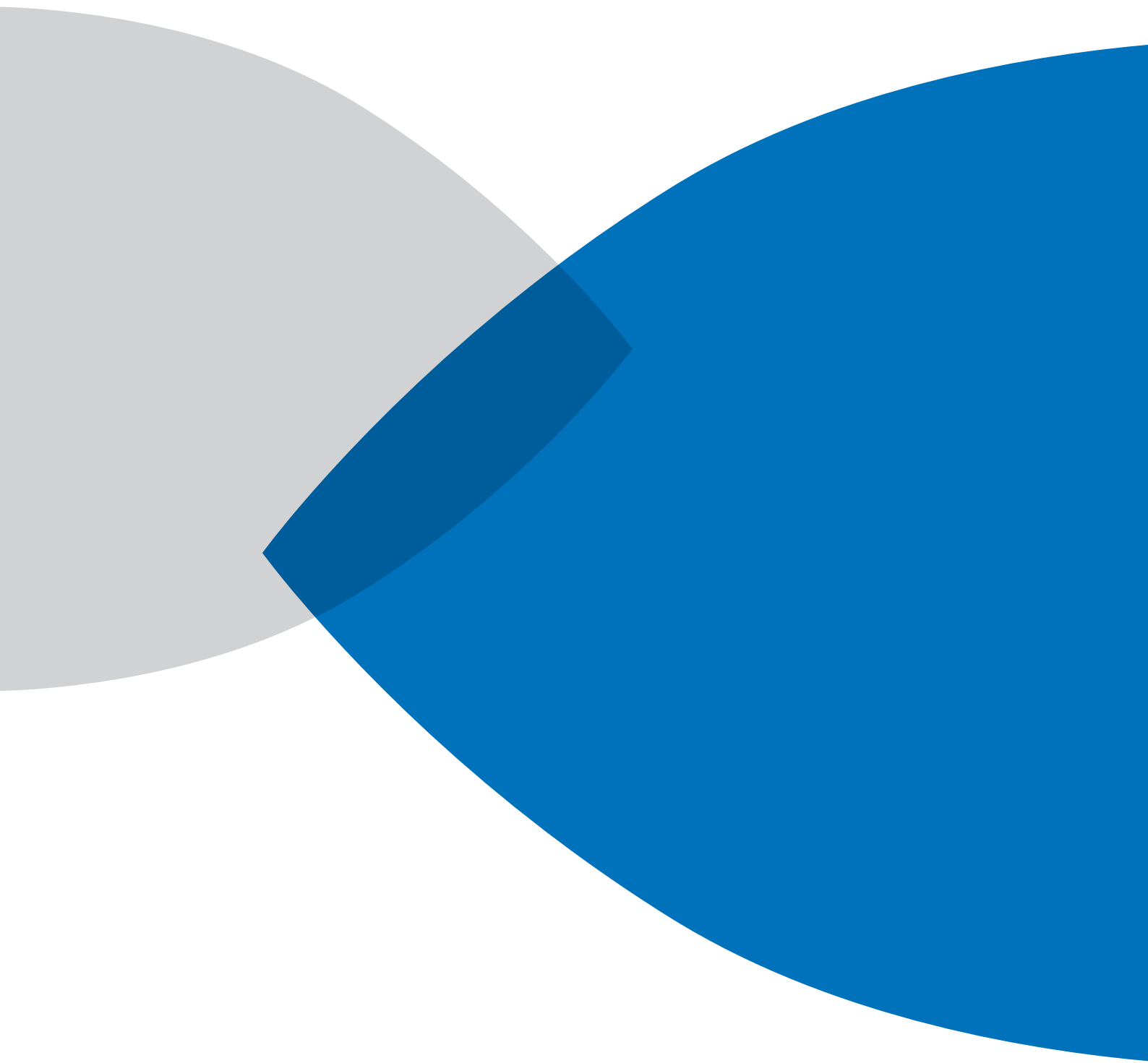
Príklad implementácie rozšírenia Distribučný systém

ČASOVANÉ AUTOMATICKÉ UZATVÁRANIE INCIDENTOV

Modul umožňuje nastaviť na úrovni Zabbix triggera dobu platnosti ním otvoreného 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 dopĺňuje 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



axians

Axians Slovakia s.r.o., Plátennícka 19013/2, 821 09 Bratislava
Tel.: +421 258 273 111, E-mail: axians@axians.sk
www.axians.sk