Open source nástroj **Zabbix** vám **pomůže ukočírovat** náklady na **IT monitoring**

Pavel Štros

Open source nástroj provozního monitoringu Zabbix je (nejen) v ČR obrovsky populární a letošní cenové přemety některých jeho komerčních alternativ tuto pozici dále posilují. Super je, že Zabbix je už přes 20 let dostupný v plné funkční výbavě zcela zdarma a nic nenasvědčuje tomu, že by se to mělo v blízké budoucnosti změnit. Za pár peněz si můžete přikoupit technickou podporu od výrobce nebo i od některého z jeho místních partnerů. Což zákazníkům doporučujeme, protože i programátoři Zabbixu musí z něčeho žít. My jako partner občas sponzorujeme vývoj některých nových funkcí, např. podpora pro jednotné přihlašování uživatelů přes SAML pro nás byla důležitá.

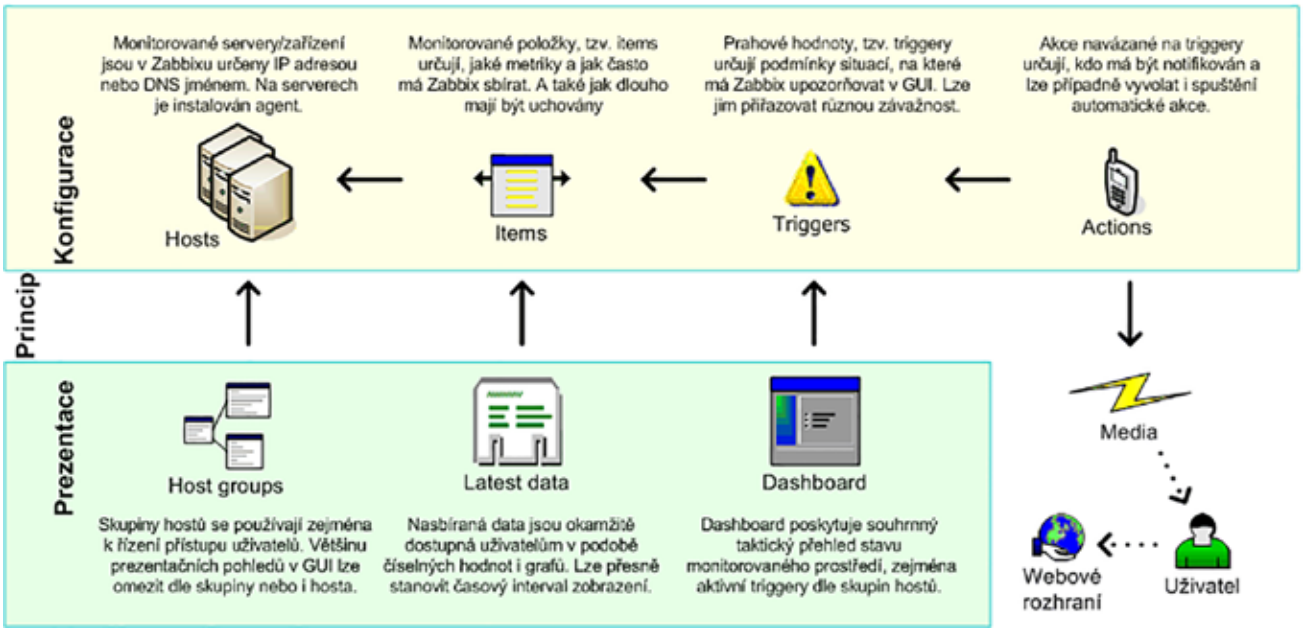
Zabbix není vhodný úplně pro každého, ovšem je dost dobrý skoro pro každého, kdo potřebuje být včas upozorněn na funkční nebo výkonové potíže monitorované IT infrastruktury. Nečekejte v Zabbixu nějaké „průvodce nastavením“. Musíte v něm sami nakonfigurovat, co žádáte sledovat a na co a jak má Zabbix reagovat. Celé se to ale dělá docela pohodlně ve webovém rozhraní a šíře výrobcem a komunitou předpřipravených šablon monitoringu pro různé technologie je opravdu veliká, viz https://www.zabbix.com/integrations.

Základní princip fungování Zabbixu je přímočarý a dlouhodobě neměnný. Potřebujete:

1. Vytvořit objekt hosta, který reprezentuje zařízení, jež potřebujete monitorovat
2. Přiřadit metriky (items), jejichž hodnoty má Zabbix o monitorovaném zařízení sbírat
3. Určit k metrikám prahové podmínky, při kterých má vznikat alarm určité závažnosti
4. Na alarmy lze dalšími podmínkami navázat reaktivní akce, nejčastěji notifikace

Výše uvedené je v Zabbixu možné snadno automatizovat různými explicitně podporovanými metodami rozkrývání zařízení v síti a přes API lze provádět i pokročilé automatizace jako navázání na změny v jednotné podnikové konfigurační databázi. Sada podporovaných metrik je velmi široká, zahrnuje všechny standardní protokoly používané pro monitoring i metriky získatelné přes multiplatformního Zabbix agenta. Výrazy stanovující prahové podmínky alarmů mohou být triviální nebo sofistikovaně komplexní a podporovány jsou i prediktivní a „anomaly“ vyhodnocovací funkce. Pro automatizované reakce jsou předpřipraveny desítky tzv. webhooků – např. pro integrace na různé tiketovací systémy.

Zjednodušeně se dá říct, že Zabbix monitoring je vhodný téměř pro každou organizaci, která spravuje více než 10 (virtuálních) serverů nebo síťových prvků. Dělali jsme instalace maličké i veliké. Zabbix nám věrně slouží při zajišťování dostupnosti služeb s ostrými SLA parametry i při monitoringu tisícovek zařízení na ministerstvech. Nemusíme řešit licencování a trápit se tím, zda konfigurací dalšího potřebného hloubkového monitoringu nepřekročíme zakoupené limity. Snad jen různí poskytovatelé obsahu a korporace mají potřebu dalších doplňků typu Prometheus a Grafana či nějakých „více byznys“ nadstaveb nad Zabbix infrastrukturním provozním monitoringem. Zabbix je svojí architekturou a bezpečnostními funkcemi dostatečně dobrý i pro silně zabezpečené systémy kritické infrastruktury státu nebo pro až paranoidně zabezpečený rozsáhlý komunikační systém provozovaný v Azure. My jsme jako partner pro tyto situace nad Zabbix vyvinuli log management a SIEM nadstavbu do jednotného řešení provozního a bezpečnostního monitoringu a služby SOC. Plus k Zabbix poskytujeme



mobilní aplikaci pro potvrzované notifikace a „svolávací“ workflow aplikaci tak, aby bylo možné v případě zjištěné havarijní situace pomocí vícekrokového a vícekanálového eskalačního procesu spolehlivě vybudit pozornost kteréhokoli z aktuálně dostupných řešitelů

A že toho Zabbix umí mnohem víc? Monitoring syntetických webových transakcí, „low level discovery“ instancí monitorovaných objektů, čím dál masivněji využívaný „item preprocesing“ apod? Ano, ale detaily se do tohoto článku prostě nevejdou. A taky jsou to pokročilejší funkce, takže pokud se neplánujete sami stát expertem na Zabbix, nejspíš si na toto už někoho najmete. Lidí s potřebnou kvalifikací je na českém trhu dostatek a plně si tak i vy můžete užívat systematicky řízeného vývojového cyklu Zabbix softwaru s dlouhodobou roadmapou a výrobcem pravidelně uvolňovanými „long term support“ verzemi.

Svoboda v kombinaci s přímočarostí konfigurace, přívětivostí uživatelského rozhraní a cenově velmi dostupnou garantovanou komerční podporou na L2 i L3 úrovni je prostě k nezaplacení!

Takže až i vy budete muset ukočírovat náklady na IT monitoring nebo budete hledat nové řešení provozního monitoringu z jiných důvodů, nemusíte nic dlouho a složitě vymýšlet. Dejte šanci Zabbixu a on vás pravděpodobně nezklame. Patří mezi nejrozšířenější bezplatné open source monitorovací systémy a poskytuje obdobné a někdy i lepší funkce než mnohá placená řešení. Mezi jeho hlavní výhody patří možnost licenčně neomezovaného sledování metrik zdraví a výkonnosti zařízení a služeb, lze ho dokonale přizpůsobit potřebám a má aktivní komunitu, která spolu s výrobcem neustále vylepšuje jeho funkcionalitu. Proto přechod na open-source řešení neznamená jen snížení nákladů, ale také získání větší kontroly nad šíří a hloubkou prováděného provozního monitoringu IT infrastruktury vašeho podniku či organizace. ■

Mgr. Pavel Štros Ph.D., CISA

Autor článku je technický ředitel firmy DATASYS.