SYSTEMY DO MONITOROWANIA BEZPIECZEŃSTWA DUŻYCH SIECI KOMPUTEROWYCH NA PRZYKŁADZIE SYSTEMU ZABBIX.

M. G T. P

Wydział Fizyki, Matematyki i Informatyki
Politechnika Krakowska im. Tadeusza Kościuszki

11.04.2019

Plan.

Wstęp.

W ostatnim czasie coraz większe znaczenie, a także popularność wśród administratorów IT, zyskują narzędzia do monitorowania sieci oraz serwerów. Tego typu oprogramowanie powinno nie tylko umożliwiać sprawdzenie (w dowolnym momencie) wykorzystania danego zasobu (np. pamięci RAM serwera), ale także wysyłać SMS-em lub e-mailem komunikaty o awarii lub wyczerpaniu zapasów mocy badanego podzespołu. Dziś tego typu systemy traktowane są już nie tylko jako przydatne narzędzia. W branży IT jest to często standard i konieczność.

Wstęp.

Potrzeba wdrożenia odpowiedniego oprogramowania spowodowała, że niezwykle popularne stały się narzędzia typu:

- Moloch
- Cacti
- Nagios
- Zabbix

Charakterystyka programu Zabbix.

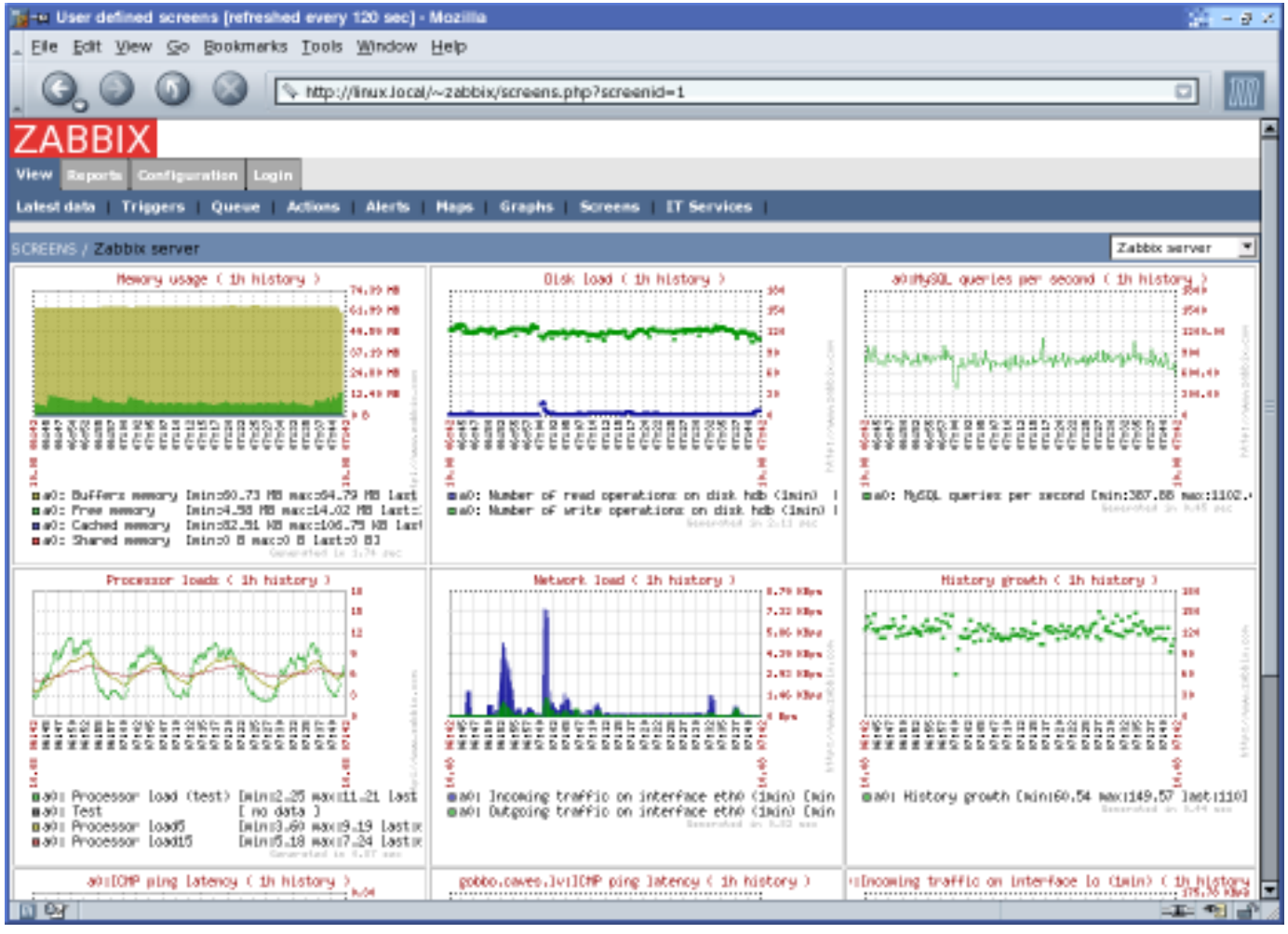
Zabbix jest systemem stworzonym przez Alexeia Vladisheva w 2001 roku. Pierwsza oficjalna i stabilna wersja pojawiła się 23 marca 2004 roku. Od 21 maja 2012 dostępna jest druga wersja systemu, który obecnie rozwijany jest przez firmę Zabbix SIA.

Charakterystyka programu Zabbix.

Za pomocą Zabbixa możemy monitorować prawie każdy parametr działania serwerów lub urządzeń sieciowych. Wspiera zarówno systemy z rodziny Windows, jak i Linux. Do jego najbardziej podstawowych funkcjonalności można zaliczyć badanie:

- wysycenia łącza sieciowego
- obciążenia parametrów serwerów
- temperatury poszczególnych podzespołów
- edycji konkretnego pliku lub folderu
- wykorzystanie baz SQL
- poprawnego wykonania zapytania SQL

Charakterystyka programu Zabbix.



Rysunek: Zabbix 1.1.6 Alpha6.

Charakterystyka programu Zabbix.

Do monitorowania wymienionych zasobów możemy wykorzystać istniejące szablony, dostępne do pobrania za darmo z Internetu, które można podpiąć do naszego systemu. Szablony to zapisany i możliwy do wyeksportowania oraz zaimportowania zestaw czujek, alarmów oraz wykresów dostosowanych do konkretnego systemu lub urządzenia. W przypadku bardziej skomplikowanych wymagań, możliwe jest podłączenie własnych skryptów. Zabbix umożliwia także monitorowanie stron WWW. Odpowiednie monitorowanie stron internetowych w Zabbixie umożliwia wysyłanie informacji do właścicieli stron WWW o problemach związanych z przerwą w działaniu lub spowolnieniu szybkości witryny internetowej.

Działanie programu Zabbix.

Zabbix umożliwia wysyłanie informacji o awarii na wiele sposobów. Do najbardziej standardowych należą informacje wysyłane drogą mailową lub SMS-em. Panel konfiguracyjny systemu posiada opcję, dzięki której możemy podłączyć naszą aplikację monitorującą do serwera SMTP. Inną, przydatną funkcją jest możliwość wykonywania pewnych akcji po wystąpieniu awarii. Możliwe jest zarówno wykonywanie określonego skryptu, jak i automatyczny restart lub uruchomienie kluczowej usługi na określonym serwerze.

Działanie programu Zabbix.

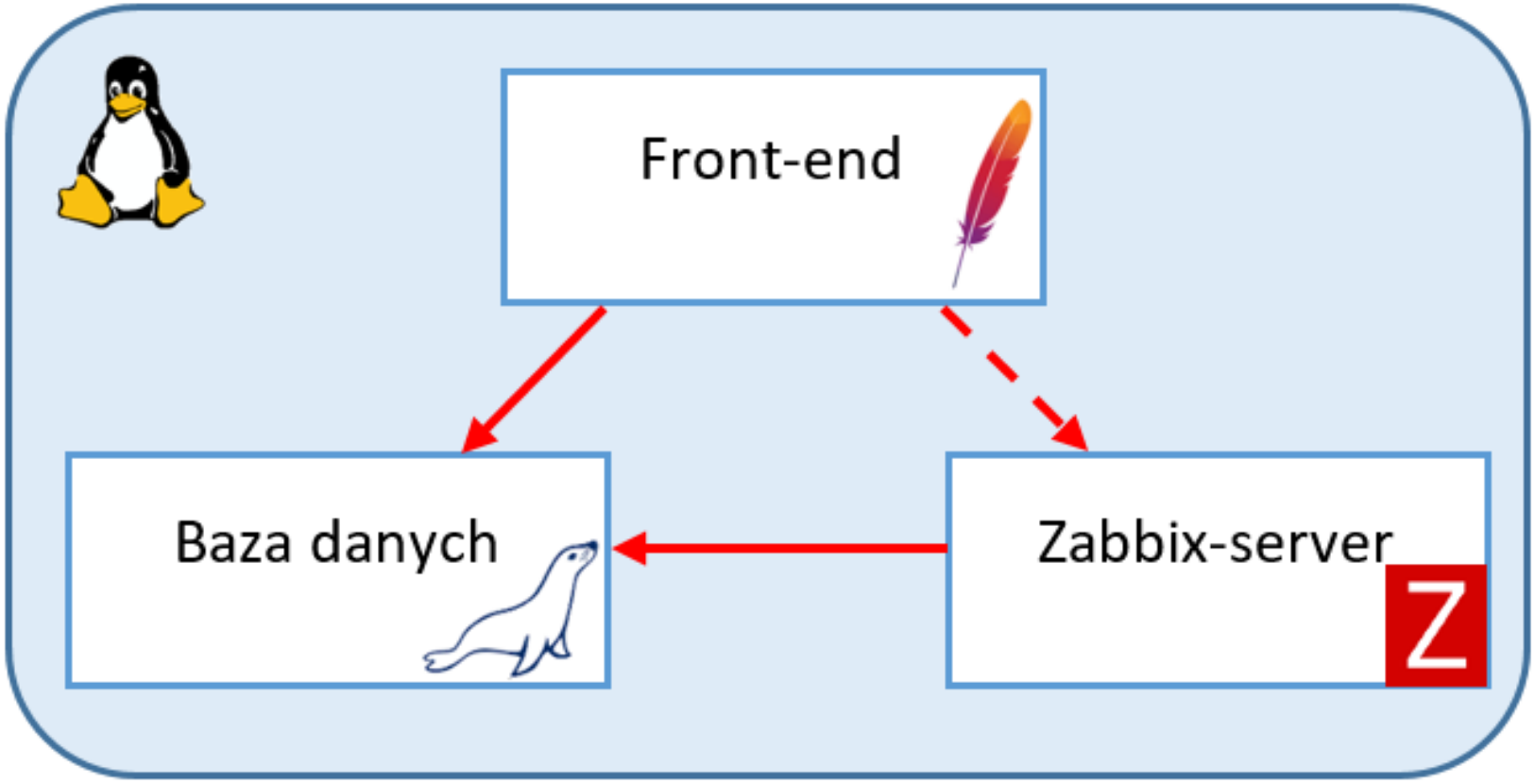
Obok tych typowych zastosowań, czyli monitoringu, Zabbix przydaje się również do analizowania ruchu w sieci. Jak już wiadomo, oprogramowanie zbiera całą masę wartościowych danych. Dzięki otrzymywanym wartościom możemy dokonywać analizy utylizacji poszczególnych zasobów w firmowej sieci. Odpowiednie wykorzystanie pozwala nie tylko zmniejszyć liczbę występujących awarii, lecz także uchronić przed wystąpieniem nowych. Stosuje się tu szacowanie wykorzystania zasobów. Oczywiście z biegiem czasu zużycie pewnych podzespołów (np. dysków) wzrasta, ale dzięki takiemu szacowaniu możemy uprzedzić moment, w którym dane zasoby ulegną wyczerpaniu.

Działanie programu Zabbix.

By móc dobrze zaplanować potrzeby naszego środowiska monitoringu, musimy znać podstawowe pojęcia związane z Zabbixem.

- **Zabbix-server** – jest to centrum oprogramowania Zabbix (właśnie ten proces odpowiada za odbiór danych, wykrywaniu anomalii, wysyłaniu powiadomień do użytkowników itp.).
- **Baza danych** – miejsce, gdzie Zabbix-server zapisuje wszystkie odebrane dane oraz wszelką konfigurację dostępną z poziomu interfejsu użytkownika.
- **Front-end** – strona WWW, gdzie użytkownik może skonfigurować wszelkie sprawdzenia oraz zwizualizować dane zapisane w bazie danych.

Działanie programu Zabbix.



Rysunek: Schemat połączeń.

Działanie programu Zabbix.

Innymi ważnymi podczas planowania pojęciami są:

- **NVPS (new values per second)** – jest to średnia liczba nowych wartości na sekundę, jakie otrzymuje Zabbix.
- **Historia** – pojedynczy wynik jednego sprawdzenia (nieważne czy jest to liczba, czy tekst) jest zapisywany jako historia.
- **Trend** – by zaoszczędzić miejsca na dysku Zabbix agreguje dane historyczne, zapisując z godziny wartości minimalne, średnie, maksymalne oraz ilość wartości w tej godzinie.
- **Zdarzenie** – głównym źródłem zdarzeń są zmiany statusu problemu (wyzwalacza); każda zmiana PROBLEM<->OK generuje zdarzenie, które przechowuje informację kiedy ona wystąpiła, czy jest potwierdzona itd.

Planowanie środowiska.

Jaka wersję Zabbix wybrać?

- **Najnowsza** – projekt Zabbix jest aktywnie rozwijany, przez co przy kolejnych wersjach twórcy przedstawiają nam wiele nowych funkcjonalności; m.in. dzięki temu również Zabbix jest szybszy poprzez ciągłą optymalizację kodu.
- **Long Term Support (LTS)** – jeżeli środowisko Zabbix ma być planowane jako bardzo krytyczne oraz stabilne, należy pomyśleć o wersji LTS.

Planowanie środowiska.

Jaką bazę danych wybrać?

Twórcy Zabbixa promują bazę MySQL wraz z silnikiem InnoDB, przez co ten typ bazy jest najlepiej udokumentowany, jak i również posiada wiele wskazówek na optymalizację (co w kwestii Zabbixa jest bardzo ważne). Jednakże można zastosować również bazę PostgreSQL czy Oracle.

Jaki front-end wybrać?

W większości przypadków wystarczy proponowane przez twórców Apache. Możemy również wybrać nginx lub Lighttpd, jednak należy brać pod uwagę że, tak samo jak w przypadku bazy PostgreSQL czy Oracle, nie są to przypadki tak dobrze udokumentowane.

Planowanie środowiska.

Jaki system operacyjny wybrać?

Linux. Są gotowe paczki (repo) dla systemów z rodziny RedHat (RHEL, CentOS, Fedora) oraz Debian i Ubuntu, ale nic nie stoi na przeszkodzie, by samemu na innym systemie skompilować Zabbixa ze źródeł. Zabbix wspiera również inne systemy UNIX np. FreeBSD. Niestety, ale Zabbix-server nie zainstalujemy na Windowsie (ale agenta do monitorowania pracy tego serwera już tak!).

Planowanie środowiska.

Jakie zasoby dobrać do serwera?

Rekomendacja twórców Zabbix.		
Wielkość	CPU/RAM	Ilość monitorowanych hostów
Małe	Virtual Appliance	100
Średnie	2 rdzenie CPU/2GB	500
Duże	4 rdzenie CPU/8GB	> 1000
Bardzo duże	8 rdzeni CPU/16GB	> 10000

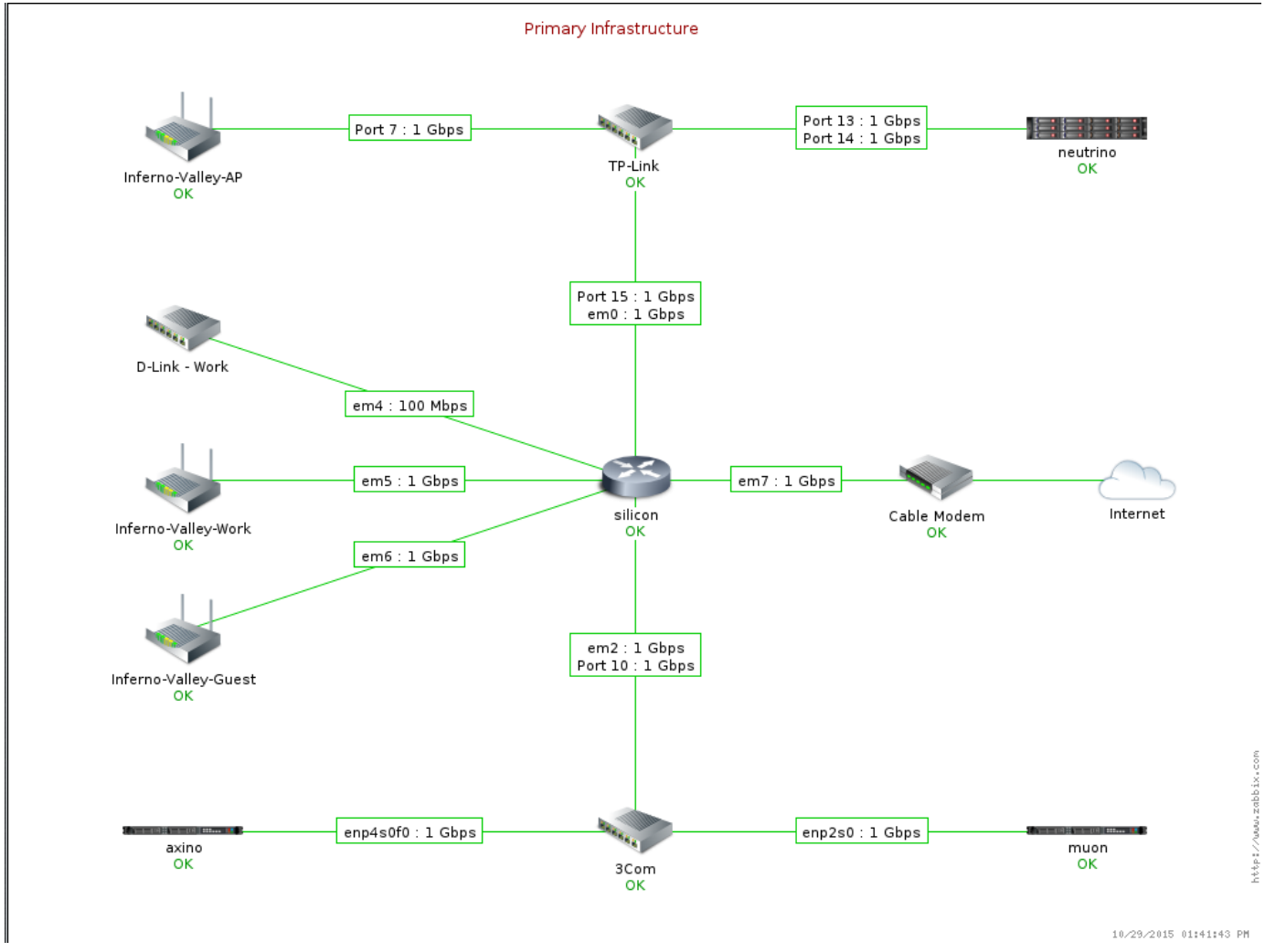
Podsumowanie - zalety.

- **Jest darmowe!** – Zabbix jest dystrybuowany na licencji GPLv2, kod oprogramowania jest ogólnie dostępny i może on być wykorzystywany do rozwiązań komercyjnych.
- **Ogrom metod monitorowania** – oprócz monitorowania hostów za pomocą natywnych agentów, możemy wykorzystać różne protokoły, m. in. SNMP, SSH, TELNET, IPMI, JPX, HTTP/HTTPS itp.
- **Stabilne oprogramowanie** – czasy młodości Zabbix ma już dawno za sobą. Dodatkowo Zabbix posiada wersje LTS (Long Time Support) która idealnie nadaje się na środowisko produkcyjne.

Podsumowanie - zalety.

- **Dobre community** – twórcy stworzyli stronę, na której ludzie mogą udostępniać swoje metody monitoringu (głównie za pomocą gotowych szablonów i skryptów). Dodatkowo twórcy udostępniają bardzo bogatą dokumentację.
- **Agregacja i wizualizacja danych** – Zabbix dobrze spisuje się jako narzędzie do zbierania danych o środowisku, aby potem móc to przedstawiać w formie wykresów czy map.

Podsumowanie - zalety.



Rysunek: Przykładowa mapa.

Podsumowanie - wady.

- **Skomplikowany interfejs.**
- **Duże zużycie zasobów.**
- **Dziury w wykresach.**

Źródła.

- https://www.zabbix.com
- https://blog.zabbix.com
- https://zabbix.org/wiki