Zabbix

Gabriela Godek i Katarzyna Olender

2 lutego 2020

Spis treści

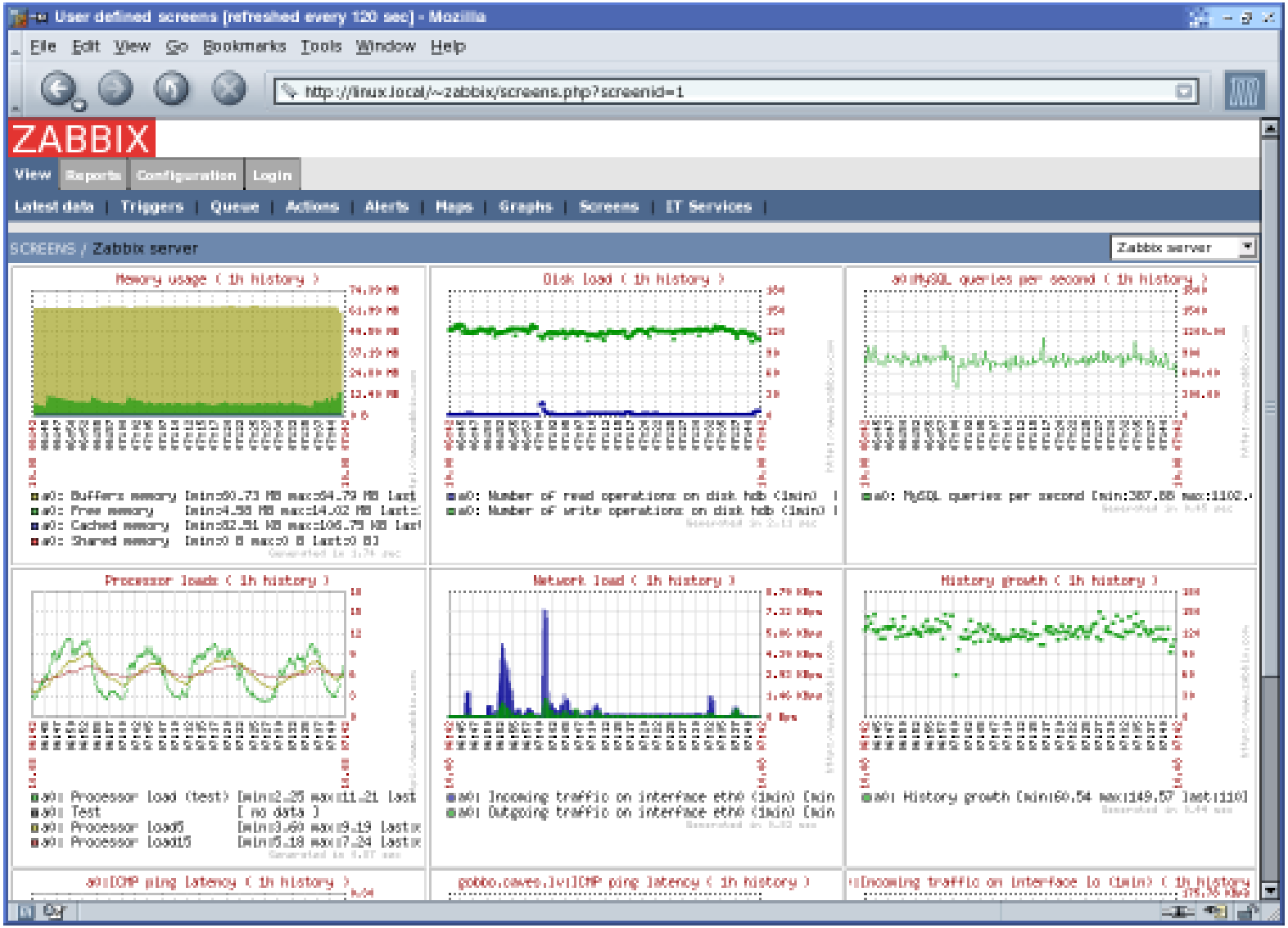
Wprowadzenie

Zabbix jest otwartym (open source) rozwiązaniem klasy enterprise - czyli jest to wyspecjalizowany system biznesowy charakteryzujący się wysoką niezawodnością, wykorzystywanym do kompleksowego monitorowania środowisk informatycznych.
Zabbix jest oprogramowaniem, które oferuje możliwość monitorowania zarówno parametrów sieci, urządzeń sieciowych, itp., jak również działania i integralności serwerów oraz usług na nich uruchomionych. Używa elastycznego mechanizmu powiadomień, pozwalającego użytkownikom skonfigurować powiadomienia e-mail dla praktycznie każdego zdarzenia

Historia

Twórca zabbixa, Alexei Vladishev, stworzył pierwszy zarys aplikacji, gdy w 1998 potrzebował narzędzia do monitoringu w firmie, gdzie pracował. Na początku były to proste skrypty napisane w perlu, jednak twórca szybko zmienił język programowania na C. Dodatkowo napisał front-end w języku PHP i w roku 2004 wypuścił pierwszą stabilną wersję – 1.0. Twórca w jednym z wywiadów opowiada również skąd się wzięła nazwa – wymyślał losowe słowa i sprawdzał w wyszukiwarce, czy są już zarezerwowane. Słowo "Zabbix" nie kryje żadnego większego znaczenia.

Historia



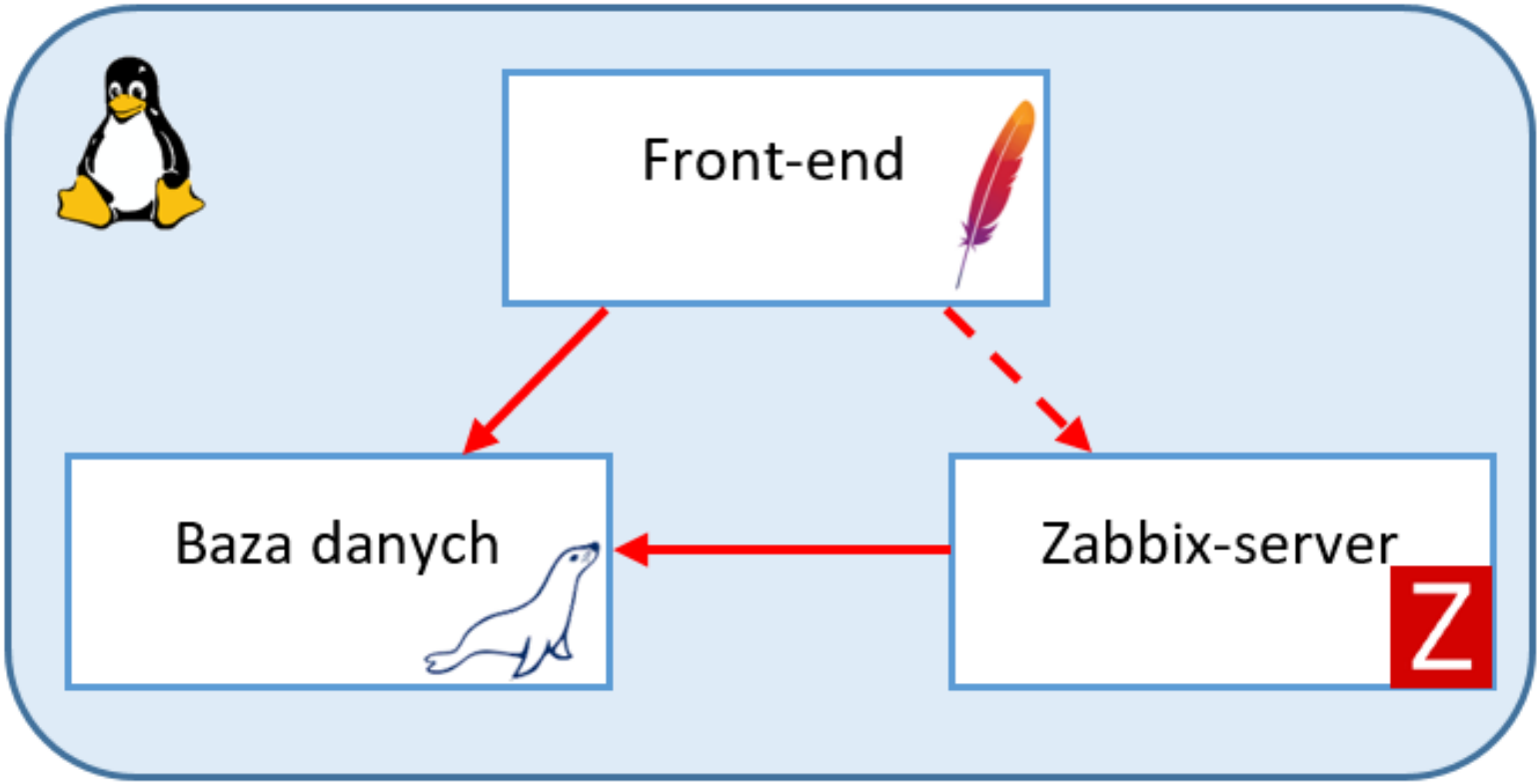
Rysunek: Zabbix 1.1.6 Alpha6 - GUI źródło: wikimedia.org

Podstawowa teoria

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.

Podstawowa teoria



Rysunek: Schemat połączeń, źródło: sekurak.pl

Licencja i dokumentacja

Zabbix, dumnie nazywany przez twórców jako **The Enterprise-Class Open Source Network Monitoring Solution**, jest rozpowszechniany na licencji GNU General Public License (GPL) v. 2. Dzięki temu można wykorzystywać go wraz z kodem źródłowym za darmo nawet w najbardziej komercyjnych technologicznie projektach. Wszystkie wersje posiadają znakomicie opisane dokumentacje, w tym dla wersji 2.2 dostępna jest ona w języku polskim. Dodatkowo Zabbix posiada wersje LTS (Long Time Support) która idealnie nadaje się na środowisko produkcyjne.

Automatyzacja

Dzięki możliwości automatyzacji pracy Zabbixa, jest on bardzo przydatny w dynamicznych, zmieniających się, dużych środowiskach.Są to między innymi następujące, wbudowane funkcje:

- **autorejestracja agentów** – automatyczne dodawanie hostów do systemu monitoringu bez konieczności ich wcześniejszej rejestracji
- **autowykrywanie obiektów w sieci** – cykliczne skanowanie wybranych segmentów sieci w poszukiwaniu hostów
- **autokonfiguracja LLD** – automatyczne dostosowanie się do zmieniającej się konfiguracji

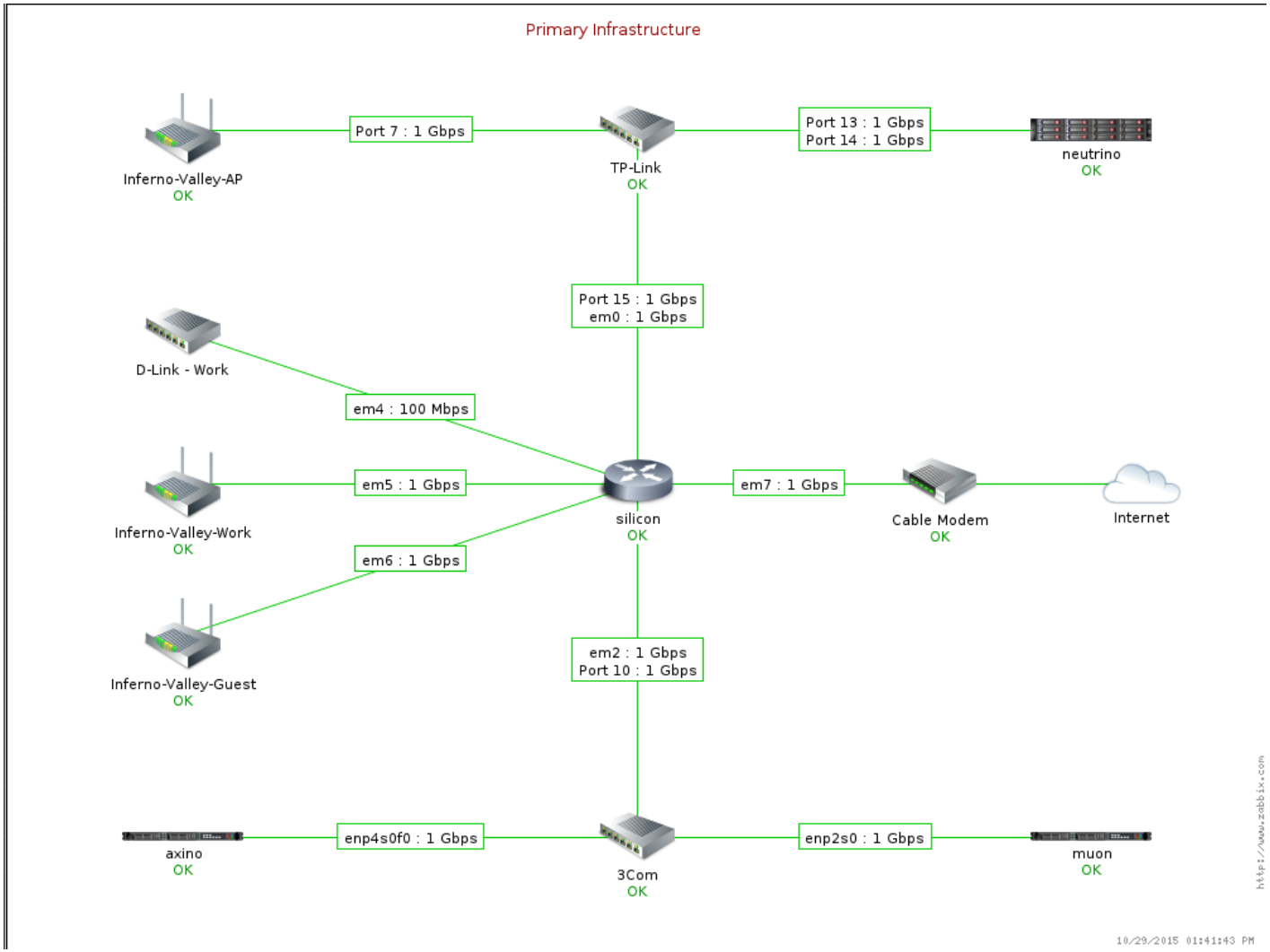
Metody monitorowania

Mamy możliwość monitorowania naszych obiektów z użyciem wielu metod i protokołów takich jak: snmp, ssh, telnet, icmp, ipmi, odbc, jmx, http, imap, smtp, ftp, dns i innych. Monitorować możemy zarówno z użyciem natywnych agentów instalowanych na systemie operacyjnym jak i bez nich. W tym ostatnim przypadku jednak będziemy ograniczeni ilością gromadzonych metryk, które daje nam tylko agent.

Wizualizacja

Gromadzone dane możemy w łatwy sposób przedstawiać na wykresie czasu. Istnieje możliwość tworzenia map ze stanem naszych obiektów oraz powiązaniami między nimi. Całość uzupełniają jeszcze różnego rodzaju raporty. Wszystkie te rzeczy możemy gromadzić w kolekcje ekranów dedykowanych pod wyświetlanie bieżących statusów.

Wizualizacja



Rysunek: Przykład mapy, źródło secretwafflelabs.com.

Rozszerzalność

Jeśli brakuje nam funkcjonalności z tych dostępnych w Zabbix to możemy w łatwy sposób ją korzystając z jednej z poniższych opcji:

- własne skrypty uruchamiane na agencie lub też bezpośrednio na serwerze
- własne skrypty LLD wykrywające nowe obiekty
- gotowe szablony dostępne na https://share.zabbix.com/

Skalowalność

Zabbix może działać w architekturze rozproszonej, gdzie występują serwery pośredniczące (proxy) buforujące dane na wypadek niedostępności serwera głównego. Zmniejszają one znacząco obciążenie serwera związaną z obsługą połączeń do obiektów jednocześnie same posiadając bardzo małe wymagania sprzętowe (możliwe jest uruchomienie serwera proxy na Raspberry PI!). Sam serwer centralny współpracuje ze znanym oprogramowaniem do klastrowania jak Pacemaker oraz konfiguracją klastrową baz danych.

Zarządzanie i integracja poprzez API

W razie potrzeby integracji istnieje możliwość wykorzystania dostępnego API. Posiada ono wsparcie wielu języków skryptowych (Python, Perl, Ruby, Powershell, Go, Java). Może być ono również wykorzystane do sprawnego zarządzania w przypadku dużej ilości obiektów jak i do dodatkowego raportowania.

Zakończenie

Wszystkie przedstawione i nieuwzględnione w prezentacji elementy połączone razem otwierają szerokie spektrum możliwości, które pozwolą na monitorowanie sieci na naprawdę wysokim poziomie.
Mamy nadzieję, że udało nam się przybliżyć Zabbixa w przejrzysty sposób.
Dziękujemy za uwagę.