Mateusz Dampc

# ZABBIX 7.0

Efektywny monitoring infrastruktury IT dla każdego

Helion

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiejkolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz wydawca dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz wydawca nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

Redaktor prowadzący: Tomasz Gojowy

Projekt okładki: Studio Gravite/Olsztyn
Obarek, Pokoński, Pazdrijowski, Zaprucki

Materiały graficzne na okładce zostały wykorzystane za zgodą Shutterstock.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
*helion.pl/user/opinie/zabbix*
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Kolorowe wersje wybranych rysunków dostępne pod adresem
*https://ftp.helion.pl/przyklady/zabbix.zip*

ISBN: 978-83-289-2060-6

Copyright © Helion S.A. 2025

Printed in Poland.

- Kup książkę
- Poleć książkę
- Oceń książkę

- Księgarnia internetowa
- Lubię to! » Nasza społeczność

# Spis treści



Kup książkę Poleć książkę

Kup książkę Poleć książkę

# Wprowadzenie

## Monitoring infrastruktury. Po co, jak i dlaczego?

W dzisiejszym świecie IT właściwie nic nie jest stałe. Postęp techniczny wymusza na dostawcach usług ciągłe ulepszenia, zmiany, aktualizacje oraz zwiększanie bezpieczeństwa urządzeń, których funkcją jest utrzymanie usług biznesowych. Często dostawcy są zmuszeni poprzez pewne regulacje rządowe lub europejskie, np. regulacje DORA czy też dyrektywy ISO, do zapewnienia, że infrastruktura będzie możliwie odporna na awarie i ataki hakerskie. Na rynku jest wiele narzędzi, które oferują zwiększenie bezpieczeństwa urządzeń w serwerowniach, jednak bardzo często są to programy bardzo drogie w utrzymywaniu i eksploatacji. Niemniej jednak certyfikat zgodności ISO 27001 pomaga przedsiębiorcom pozyskiwać nowych klientów. Dlatego aby móc spełniać owe wymogi, trzeba również wprowadzić monitoring infrastruktury.

Monitoring bardzo często kojarzy się z kamerami cyfrowymi montowanymi na budynkach. Oczywiście nie jest to błąd — to zastosowanie należy do szerokiej gamy pojęć, które się kryją pod słowem „monitoring". Tak jak kamery obserwują otoczenie budynków, tak wyspecjalizowane narzędzia weryfikują stan sieci, serwerów czy też aplikacji. Każdy niepożądany stan, który powoduje przerwy w działaniu, trzeba jak najszybciej zmienić na pożądany, aby nie dopuścić do strat finansowych. Niejedna firma w XXI wieku przez drobne problemy, drobne niedopatrzenie musiała płacić gigantyczne odszkodowanie, które wiele z nich doprowadziło do upadku. Dobrym przykładem takiej sytuacji jest przypadkowe wykrycie podatności w protokole SSH (CVE-2024-3094), potocznie nazywanej podatnością XZ. W skrócie podatność polegała na tym, że podczas nawiązywania sesji przez OpenSSH uruchamiały się zarchiwizowane testy, które miały na celu przesłanie wprowadzonych danych logowania na zewnętrzne serwery. Ów problem był na tyle krytyczny, że mógł zagrozić bezpieczeństwu wielu krajów. Był też na tyle istotny, że występował już w wersjach systemów operacyjnych, które niebawem miano wydać. Na szczęście udało się w porę (przypadkiem) go wykryć i wyeliminować zagrożenie. Cała sytuacja pokazuje, jak niewiele brakowało, aby udostępnić dane logowania niepożądanym osobom.

Innym przykładem zastosowania monitoringu chroniącego przed podatnościami jest sprawdzanie wersji aplikacji Java, które bardzo często stosuje się w firmach. Do popularnych narzędzi wykorzystujących język programowania Java należą choćby: ELK stack, Apache Tomcat, Cassandra, Jenkins czy też Zabbix Java Gateway, dokładnie omówiony w rozdziale dotyczącym tej usługi. W 2021 roku wykryto podatność

Kup książkę Poleć książkę

CVE-2021-44832 (potocznie nazywaną podatnością Log4j), która polegała na możliwości zdalnego wykonania złośliwego kodu z uprawnieniami administratorskimi bez konieczności logowania. Już sam opis brzmi złowrogo. Wykryto ją w licznych aplikacjach wykorzystujących Javę, dlatego wiele firm zdecydowało się na aktualizację narzędzi, które zawierały poprawki usuwające tę podatność. W małych organizacjach problem nie był duży: kilka serwerów, narzędzi — i gotowe. Natomiast w przypadku średnich i dużych problem narastał. Duża liczba serwerów oraz aplikacji, a bardzo często również mocno rozbudowany podział odpowiedzialności powodowały chaos. Programiści z własnymi serwerami mogli nie wiedzieć, co dokładnie na nich instalowali na potrzeby testów, a administratorzy nadzorujący całe środowiska często nie wiedzieli, co instalowali użytkownicy serwerów, z powodu dużej skali infrastruktury. Działy zarządzające bezpieczeństwem nakazują jak najszybsze łatanie „dziur" — reagować trzeba bezzwłocznie. Tylko skąd wiadomo, gdzie jest zainstalowane oprogramowanie, które ma lukę bezpieczeństwa? Na ilu serwerach? Bez zweryfikowania wersji komponentów i zebrania informacji o nich nigdy nie wyeliminuje się problemu.

Skuteczny monitoring pozwala na wczesne wykrywanie niepożądanych wersji pakietów i systemów, które mogą wywołać różne incydenty. Nawet jeśli monitoring działa post factum, to wciąż może wskazać dotknięte problemem serwery, który trzeba jak najszybciej wyeliminować, aby nie narazić organizacji na straty finansowe, wizerunkowe oraz prawne, a przede wszystkim — na sam wyciek danych. Utrzymanie czytelnego inwentarza, konfiguracji oraz powiadomień może szybko zwiększyć efektywność usług, które dana firma oferuje swoim kontrahentom, a administratorom zarządzającym serwerownią zapewni spokojny sen i poczucie bezpieczeństwa w utrzymywanym środowisku oraz ułatwi jego utrzymanie.

Kolorowe wersje wybranych rysunków dostępne pod adresem
*https://ftp.helion.pl/przyklady/zabbix.zip*

## Czym jest Zabbix?

Do skutecznego monitorowania infrastruktury IT na dzisiejszym rynku potrzeba oprogramowania, które obsługuje szeroką gamę protokołów, od Telnetu poprzez HTTP aż do własnych typów komunikacji, takich jak skrypty czy specjalne narzędzia pomocnicze. Bardzo duża część programów monitorujących jest przeznaczona do wyspecjalizowanych urządzeń lub konkretnych zastosowań. Na przykład:

- Cisco Prime — jest oprogramowaniem do zarządzania konfiguracją urządzeń Cisco oraz ich monitorowani,
- The Dude — zajmuje się monitoringiem urządzeń z rodziny Mikrotik,
- Prometheus — skupia się na środowisku osadzonym, takim jak kontenery i systemy operacyjne,
- Graylog — zbiera dane tekstowe i analizuje je pod różnym kątem,

Kup książkę Poleć książkę

- Observium — skupia się na monitoringu sieci komputerowych,
- Whatsup Gold — jest płatnym oprogramowaniem do monitorowania serwerów i urządzeń sieciowych.

Z powyższych przykładów można wywnioskować, że na rynku IT funkcjonuje bardzo duża liczba programów, z których użyciem można zapewnić zgodność z procedurami i dyrektywami. Jednak stosowanie dużej liczby narzędzi powoduje chaos w kwestiach zarządzania oraz utrzymania. Przy tym często koszt licencji na tego rodzaju oprogramowanie jest bardzo wysoki, przez co niektórych instytucji nie stać na zakup takich specjalistycznych systemów. Z pomocą przychodzi rozwiązanie oparte na otwartym kodzie, takie jak Zabbix.

Jest to uniwersalne i darmowe narzędzie do monitoringu klasy korporacyjnej, dzięki któremu możemy sprawdzać i kolekcjonować dane z niemalże każdego systemu informatycznego, bez względu na jego rodzaj. Zgodnie ze słowami twórcy oprogramowania i założyciela firmy Aleksieja Władyszewa (Alexiei Vladishev), Zabbix potrafi kolekcjonować metryki z każdego miejsca, z którego można zebrać dowolną wartość liczbową bądź tekstową[1]. Takie podejście pozwala na monitorowanie w zasadzie wszystkiego, co jest dostępne w IT, a nawet OT. Zabbix pozwala na bardzo wydajne i efektywne monitorowanie serwerów fizycznych oraz wirtualnych, urządzeń sieciowych, chmury, szerokiej gamy aplikacji, urządzeń IoT, kontenerów, a także usług biznesowych. Szerokie zastosowanie tego narzędzia umożliwia komplementarne zarządzanie ryzykiem i bezpieczeństwem firm.

Do podstawowych zadań wykonywanych przez Zabbixa wliczają się:

- kolekcjonowanie metryk,
- wizualizacje,
- powiadomienia o problemach,
- automatyzacja,
- przechowywanie uzyskanych wartości w relacyjnej bazie danych.

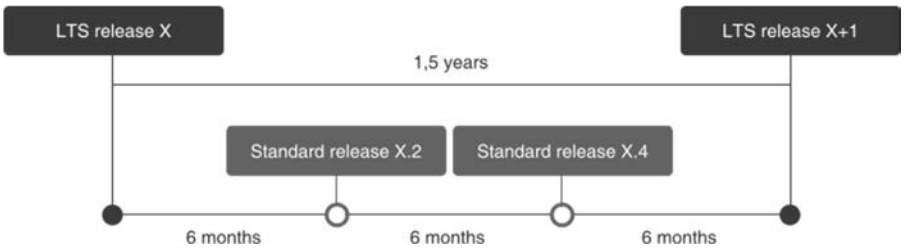
Pierwsze stabilne wydanie Zabbixa jako narzędzia do monitorowania infrastruktury IT ujrzało światło dzienne w 2004 roku i wciąż regularnie zyskuje on nowe funkcjonalności. 4 czerwca 2024 roku udostępniono wersję 7.0 LTS (ang. *Long Term Support*), wprowadzającą w porównaniu z wersją 6.0 LTS szereg nowych funkcjonalności, m.in.:

- asynchroniczne procesy zbierające metryki z urządzeń końcowych,
- możliwość zwiększenia limitu czasu per pozycja,
- możliwość rozszerzenia wysokiej dostępności rozwiązania na podstawie grup Zabbix proxy,
- możliwość uruchamiania skryptów na urządzeniach końcowych z własnymi parametrami w językach zrozumiałych dla systemu operacyjnego, takich jak PowerShell, Bash, Python itd.,

[1] Aleksiej Władyszew, *Re-thinking Zabbix*, Zabbix Summit, Ryga 2022, *https://youtu.be/4FLEN7KuQ8w?si=0B_tWhB7_nh75hpn&t=1144*.

Kup książkę Poleć książkę

- zwiększenie wydajności w kolekcjonowaniu metryk oraz działaniu frontendu,
- dodatkowe widżety wizualizacyjne,
- weryfikację dostępności nowszych wersji oprogramowania,
- zarządzanie użytkownikami z poziomu zewnętrznego systemu Active Directory,
- monitoring stron WWW z wykorzystaniem silnika przeglądarkowego,
- wsteczną kompatybilność z Zabbix proxy.




**RYSUNEK W.1**. Polityka wydawania nowych wersji Zabbixa[2]

Polityka wydawania nowych wersji systemu Zabbix jest następująca (rysunek W.1):

- Wersje LTS (ang. *Long Term Support*) wydawane są co 1,5 roku. Wersje LTS uzyskują pełne wsparcie produktu w postaci poprawek kodu i usuwania podatności przez 5 lat od wydania wersji LTS (3 lata pełnego wsparcia, 2 lata ograniczonego). Charakteryzują się zerem na drugim miejscu po oznaczeniu wersji głównej, np. 4.0, 5.0., 6.0, 7.0, 8.0 itd.
- Wersje pośrednie (standardowe) to wersje wydawane pomiędzy systemami LTS. Charakteryzują się utrzymaniem wsparcia do czasu wydania kolejnej stabilnej wersji (średnio co 6 miesięcy). W momencie opublikowania nowszego wydania można liczyć również na 6-miesięczne ograniczone wsparcie w postaci usuwania krytycznych podatności. Zaleca się aktualizowanie Zabbixa do najnowszej dostępnej wersji. Wersje pośrednie charakteryzują się parzystym oznaczeniem na drugim miejscu po oznaczeniu wersji głównej, np. 4.2, 6.4, 7.2 itd.
- Wersje testowe (niestabilne) to wersje oprogramowania niezalecane do uruchamiania w środowisku produkcyjnym. Są to wersje deweloperskie, niestabilne, pozbawione wsparcia producenta. Charakteryzują się nieparzystym oznaczeniem na drugim miejscu po oznaczeniu wersji głównej, np. 6.1, 6.3:
  - x.1 oznacza wersję alfa lub beta wydaną przed wersją x.2,
  - x.3 oznacza wersję alfa lub beta wydaną przed wersją x.4,
  - x.5 oznacza wersję alfa lub beta wydaną przed wersją LTS x+1.0.

Oznacza to, że od ponad 20 lat produkt nieustannie prężnie się rozwija, zyskuje nowe funkcjonalności oraz obsługuje coraz to nowsze protokoły komunikacyjne. Do każdej zebranej wartości można przygotować osobny wykres bądź wyzwalacz, który

[2] Źródło: *https://www.zabbix.com/life_cycle_and_release_policy/*; dostęp 15.11.2024.

Kup książkę Poleć książkę

będzie sygnalizować odchylenie danej od określonego wcześniej progu. To wszystko pozwala administratorom działać proaktywnie. Problemy można w ten sposób naprawić przed zgłoszeniem przez klienta, a jeśli niepożądana sytuacja jest trywialna, schematyczna bądź występuje cyklicznie, problem mogą rozwiązać automatyczne akcje wyzwalane przez system monitoringu.

Zabbix jako narzędzie wykorzystywane w IT oraz OT sprawdzi się w każdej instytucji, branży czy też w środowisku domowym. Stosuje się go na całym świecie, niemalże w każdej dziedzinie. Dla przykładu, używa go Europejska Agencja Kosmiczna do monitorowania Międzynarodowej Stacji Kosmicznej, jest też obecny w takich firmach jak Dell (branża IT), Orange (branża telekomunikacyjna) i Seat (branża automotive)[3].

Zabbix do monitoringu wykorzystuje takie rozwiązania jak:

- protokół SNMP/ pułapki SNMP,
- protokół Telnet,
- SSH,
- silniki ODBC do odpytywania baz danych,
- protokół IPMI,
- protokół ICMP,
- protokoły HTTP/HTTPS,
- protokół Modbus,
- protokół MQTT,
- JavaScript,
- własny protokół oparty na JSON — Zabbix agent oraz Zabbix sender,
- i cokolwiek innego, co wykorzystuje skrypty napisane w języku zrozumiałym dla serwera, na którym są uruchamiane.

Elastyczność rozwiązania wspomaga organizacje w zarządzaniu swoją infrastrukturą, zasobami i usługami biznesowymi, realnie wpływając na dochody firmy oraz zapobiegając utracie wiarygodności w oczach kontrahentów.

Zabbix jest również bardzo dobrym integratorem z innymi systemami, gdyż pozwala na automatyzację pracy z wykorzystaniem m.in. zgłoszeń, zdalnych poleceń czy powiadomień użytkowników. W sektorze IT firmy bardzo często stosują metodyki pracy ITIL, dlatego narzędzia do monitoringu powszechnie wykorzystuje się do raportowania incydentów w różnych systemach ticketowych, takich jak Jira, ServiceNow, Manage Engine Service Desk Plus, Gitlab czy też Zammad. Umożliwia to instytucjom pracę w metodyce opartej na zgłoszeniach we w pełni zautomatyzowany sposób, gdyż Zabbix pozwala na utworzenie incydentu w systemie natychmiast po wykryciu problemu. Analogicznie działa to w przypadku powiadomień mailowych, esemesowych czy też z wysyłką bezpośrednio na czat, np. Discord, Jabber, Slack, Telegram lub Skype. W powiadomieniach można także tworzyć integracje z własnymi systemami zarządzania, z użyciem webhooków napisanych w języku JavaScript bądź skryptów alarmowych napisanych przez administratorów.

[3] Źródło: *https://www.zabbix.com/*, *https://www.zabbix.com/users*.

Kup książkę Poleć książkę

Mówiąc o integracjach, nie sposób nie wspomnieć o tym, że Zabbix ma swoje własne API, którego można używać do kreowania własnych raportów lub integracji z systemami wizualizacji, takimi jak Grafana. Odpowiednio skonfigurowane środowisko z wizualizacjami pozwoli zidentyfikować problem w bardzo krótkim czasie. Oprogramowanie Grafana utrzymuje własny plugin wykorzystujący API Zabbixa do komunikacji bezpośrednio z systemem monitorującym i wyświetlania danych. Jest to dobra alternatywa dla wbudowanych w Zabbix frontend pulpitów, gdyż Grafana pozwala na integrację z innymi źródłami danych na jednym, przeznaczonym do tego widoku.

## Definicje

Przed szczegółowym omówieniem wszystkich komponentów, elementów oraz schematów działania należy przedstawić i wytłumaczyć pojęcia, które będą omawiane. Każdy z elementów uwzględnionych w tabeli W.1 zostanie szerzej omówiony bądź wspomniany przynajmniej w jednym podrozdziale.

**TABELA W.1.** Definicje elementów wykorzystywanych w systemie Zabbix w języku polskim i angielskim

| POLSKA NAZWA | NAZWA ANGIELSKA | OPIS |
|---|---|---|
| Zabbix serwer | Zabbix Server | Jeden z trzech głównych komponentów środowiska Zabbix. Odpowiada za wykrywanie problemów, powiadamianie oraz kolekcjonowanie metryk z infrastruktury |
| Zabbix frontend | Zabbix Frontend | Jeden z trzech głównych komponentów środowiska Zabbix. Odpowiada za wszelką wizualizację, od zarządzania konfiguracją monitoringu po wyświetlanie zebranych danych na wykresach i pulpitach |
| Baza danych Zabbixa | Zabbix database | Relacyjna baza danych, w której są przechowywane dane konfiguracyjne oraz dane z zebranych metryk. Trzeci najważniejszy komponent środowiska Zabbix |
| Zabbix proxy | Zabbix Proxy | Oprogramowanie dodatkowe wspomagające Zabbix serwer w kolekcjonowaniu metryk ze zdalnych lokalizacji oraz w przetwarzaniu wstępnym uzyskanej wartości |
| Zabbix agent | Zabbix Agent | Narzędzie instalowane na urządzeniach końcowych z systemem operacyjnym Linux, macOS lub Windows. Odpowiada za kolekcjonowanie metryk i wysłanie danych do Zabbix serwera lub Zabbix proxy. Dostępne w dwóch wariantach: Zabbix agent oraz Zabbix agent 2 |
| Host | Host | Logiczna reprezentacja monitorowanego elementu. Może to być serwer, stacja robocza, aplikacja, strona internetowa, baza danych bądź dowolny element, który ma być sprawdzany |

Kup książkę Poleć książkę

**TABELA W.1.** Definicje elementów wykorzystywanych w systemie Zabbix w języku polskim i angielskim (ciąg dalszy)

| POLSKA NAZWA | NAZWA ANGIELSKA | OPIS |
|---|---|---|
| Grupa hostów | Host group | Logiczna reprezentacja danego zbioru hostów, np. *Serwery*, *Stacje robocze*, *Aplikacje*, *Strony internetowe*, *Bazy danych* itp. |
| Pozycja | Item | Element określający, co ma zostać zebrane z hosta. Na przykład:<br>♦ pozycja typu *Agent Zabbix* zdefiniowana pod kluczem `system.cpu.util` zwróci procent wykorzystania procesora z hosta, na którym zainstalowano Zabbix agenta,<br>♦ pozycja typu *Proste sprawdzenie* zdefiniowana pod kluczem `icmpping` zwróci wartość `1`, gdy urządzenie odpowie na żądanie protokołu ICMP, bądź `0`, gdy odpowiedź będzie negatywna |
| Przetwarzanie wstępne | Preprocessing | Modyfikuje wartość otrzymaną przez Zabbix serwer lub Zabbix proxy zgodnie z regułami zdefiniowanymi dla danej pozycji |
| Wyzwalacz | Trigger | Definicja wyrażenia opartego na jednej bądź wielu funkcjach matematycznych. Określa stan problemu na podstawie danych uzyskanych przez podane pozycje. Przykładowo niepożądaną sytuacją może być utrzymująca się od 5 minut wartość `0` z pozycji o kluczu `icmpping`, oznaczająca niedostępność hosta (`/host/icmpping.max(5m)=0`) |
| Wykres | Graph | Wizualizacja graficzna na Zabbix frontendzie danych otrzymanych przez pozycje w podanym okresie |
| Pulpit | Dashboard | Zbiór widżetów wizualizujących w różnej formie dane otrzymane przez pozycje na jednym, oddzielnym widoku |
| Reguła wykrywania niskopoziomowego | Low Level Discovery | Zbiór prototypów pozycji, wyzwalaczy, wykresów oraz hostów, który na podstawie otrzymanych obiektów w liście JSON sprawia, że Zabbix serwer automatycznie tworzy elementy wykorzystywane w monitoringu |
| Scenariusz sieci WWW | WWW | Monitoring wykorzystujący bibliotekę `libcurl` do monitorowania wydajności i dostępności stron internetowych. Nie obsługuje JavaScriptu |
| Szablon | Template | Zbiór elementów takich jak pozycje, wyzwalacze, reguły wykrywania niskopoziomowego czy scenariusze sieci WWW, które mają zostać przypisane do hostów |
| Grupy szablonów | Template groups | Logiczna reprezentacja danego zbioru szablonów, np. *Szablony serwerowe*, *Szablony serwerowe/ Windows*, *Szablony aplikacyjne*, *Szablony bazodanowe*, *Szablony sieciowe* itp. |

Kup książkę Poleć książkę

**TABELA W.1.** Definicje elementów wykorzystywanych w systemie Zabbix w języku polskim i angielskim (ciąg dalszy)

| POLSKA NAZWA | NAZWA ANGIELSKA | OPIS |
|---|---|---|
| Usługa | Service | Funkcja w Zabbixie służąca do obliczania stanu dostępności poziomu usług biznesowych (SLA). Na podstawie wygenerowanych przez wyzwalacze problemów weryfikowana jest dostępność komponentów infrastruktury, które mogą wspomagać firmy przy rozliczaniu usług sprzedawanych kontrahentom |
| Znacznik | Tag | Oznaczenie hosta, szablonu, pozycji, wyzwalacza, scenariusza sieci WWW bądź usługi zgodnie z przyjętymi kryteriami, np. znacznik *Środowisko* o wartości *Produkcyjne* lub *Testowe* |
| Zdarzenie | Event | Sytuacja wygenerowana przez zmianę stanu wyzwalacza, np. z `Problem` na `OK`. Zdarzenie pełni funkcję identyfikatora problemu |
| Akcja | Action | Oparty na zdarzeniu zbiór warunków, które muszą być spełnione, aby uruchomiło się automatyczne powiadomienie |
| Operacja | Operation | Zdefiniowane reguły powiadomienia po spełnieniu warunków akcji, np. wysłanie powiadomienia mailowego do grupy użytkowników |
| Wykrywanie | Discovery | Reguła pozwalająca na wykrywanie urządzeń w infrastrukturze informatycznej oparte na zakresach adresacji IP |
| Automatyczna rejestracja Zabbix agenta | Active agent autoregistration | Akcje automatycznych działań wykonywanych przez Zabbixa w momencie otrzymania informacji o pojawieniu się nowego hosta, na którym poprawnie zainstalowano Zabbix agenta w trybie aktywnym |

## Standardowa architektura

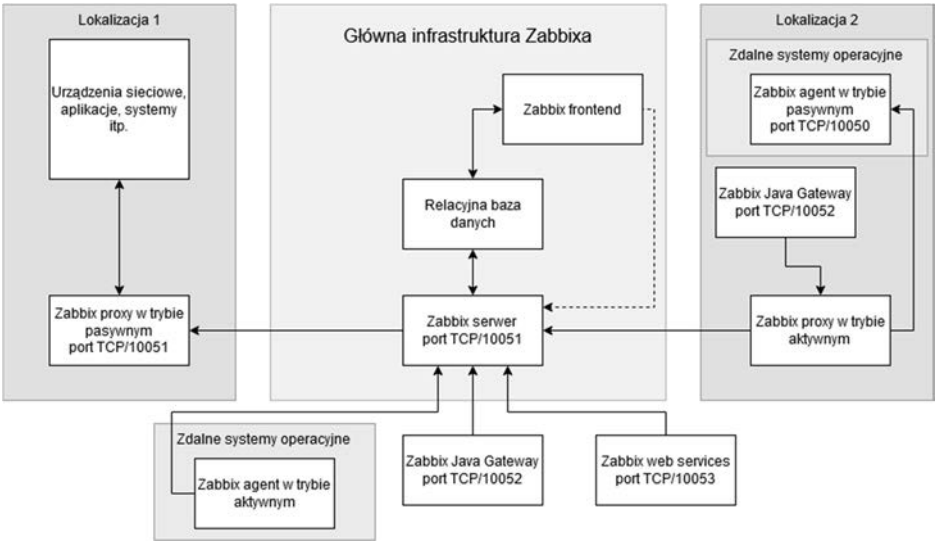
Głównymi komponentami systemu Zabbix są:

- usługa `zabbix-server` zainstalowana na serwerze z systemem operacyjnym Linux,
- usługa WWW utrzymująca Zabbix frontend,
- relacyjna baza danych (zazwyczaj MySQL lub PostgreSQL).

To zbiór tych trzech komponentów nazywamy „Zabbixem", gdy mamy na myśli całe narzędzie monitorujące. Każdy z tych komponentów może być zainstalowany na osobnym serwerze oraz być sklastrowany w taki sposób, aby zapewnić jak największą dostępność całego systemu.

Kup książkę Poleć książkę

Na rysunku W.2 jest pokazany schemat połączeń pomiędzy komponentami systemu monitorowania.




**RYSUNEK W.2.** Diagram przedstawiający połączenia pomiędzy komponentami Zabbixa

Zabbix serwer jako komponent centralny odgrywa rolę integratora z innymi systemami. Aczkolwiek nie może on działać prawidłowo bez relacyjnej bazy danych, z której pobiera informacje o całej konfiguracji monitoringu, czyli wszystkich hostach, pozycjach, wyzwalaczach, regułach wykrywania itd. Połączenie z bazą danych służy również do wprowadzania danych pobranych z urządzeń końcowych poprzez pozycje lub zdalnych Zabbix proxy, zainstalowanych w innych lokalizacjach. Dlatego ta komunikacja musi zostać zachowana i być zawsze dostępna.

Następnym elementem jest Zabbix frontend. Na diagramie pokazanym na rysunku W.2 widać charakterystyczną linię przerywaną pomiędzy nim a Zabbix serwerem, dlatego że połączenie to służy tylko w kilku sytuacjach, takich jak:

- przeglądanie kolejki na Zabbix serwerze,
- zwracanie informacji, czy Zabbix serwer jest uruchomiony,
- możliwość wykonania przycisku *Test* na wybranych pozycjach,
- możliwość uruchomienia skryptu frontendowego.

Zabbix frontend zarządza konfiguracją monitoringu, która jest bezpośrednio zapisywana w bazie danych. Zapisane dane mogą zostać wykorzystane przez usługę WWW do zwizualizowania danych historycznych z danego urządzenia w taki sposób, że każdy wprawiony administrator lub użytkownik zweryfikuje, czy w wybranym czasie jego systemy działały poprawnie.

Komponentem wspierającym główną architekturę jest usługa Zabbix proxy, która służy m.in. do odciążenia głównego systemu w kolekcjonowaniu metryk z urządzeń końcowych, głównie w momencie, gdy ma być monitorowana infrastruktura

Kup książkę Poleć książkę

umieszczona w innej lokalizacji niż system utrzymujący Zabbix serwer. Wykorzystanie Zabbix proxy jest dobrą praktyką pozwalającą na zwiększenie wydajności całego systemu. Tę tezę potwierdza również to, że jeden Zabbix serwer może obsłużyć nieograniczoną liczbę proxy.

Zabbix agent jest komponentem, który zainstalowany na urządzeniu z systemem z rodzin Linux, macOS lub Windows jest w stanie zebrać szereg informacji o tym hoście. Może działać w dwóch trybach (tak jak Zabbix proxy): aktywnym (host wysyła dane do kolekcjonera danych) i pasywnym (host otrzymuje żądanie o przesłanie wartości z kolekcjonera danych). Oprogramowanie to może wysyłać wartości bezpośrednio do Zabbix serwera lub Zabbix proxy. Obszerniej Zabbix agent jest omówiony w poświęconym mu rozdziale.

Zabbix Java Gateway stosuje się wtedy, gdy w danej infrastrukturze wymagane jest monitorowanie aplikacji, która wykorzystuje język Java. Zabbix używa rozszerzenia do Javy o nazwie Java Management Extensions (JMX). Pozycja stosująca monitoring oparty na JMX odwołuje się do obiektów `mbean`, aby wyciągnąć dane bezpośrednio z samej aplikacji. Do jednego Zabbix serwera można przypisać tylko jeden Zabbix Java Gateway. W momencie gdy wymagana jest rozbudowa środowiska o kolejny *gateway*, należy zastosować usługę Zabbix proxy, która będzie używać dodatkowego komponentu.

Na sam koniec zostaje usługa Zabbix web service, która pomimo swojej nazwy nie pełni żadnej funkcji związanej z dostępnością strony WWW. Jest to dodatkowy i całkowicie opcjonalny komponent, który odpowiada za tworzenie oraz wysyłanie raportów mailowych z załącznikiem w formacie PDF. Komponent ten otrzymuje sygnał od Zabbix serwera z wymogiem utworzenia raportu w pliku *.pdf* opartego na pulpitach znajdujących się na Zabbix frontendzie. W tym celu Zabbix web service wykorzystuje silnik przeglądarkowy, np. Google Chrome, aby wykonać zrzut ekranu podanego pulpitu, i przesyła zawartość z powrotem. Następnie dzięki swoim możliwościom alarmowania Zabbix serwer wysyła taki raport do adresatów podanych w konfiguracji raportu cyklicznego we frontendzie.

## Zabbix Cloud

Podczas wydarzenia „Zabbix Summit 2024” w Rydze zaprezentowano nowy produkt — Zabbix Cloud. Jest to pełne środowisko monitoringu dostępne na serwerach Zabbix, uruchamiane w modelu płatnej subskrypcji, w którym płaci się za wykorzystane zasoby sprzętowe. Można je w dowolnej chwili skalować, aby zwiększyć bądź zmniejszyć wydajność systemu. Ten sposób zapewnia m.in. wsparcie producenta oraz zawsze najnowszą wersję systemu. Jest to bardzo dobre rozwiązanie dla firm, które nie mają pracowników o umiejętnościach w administrowaniu systemami z rodziny Linux. W ten sposób uruchamia się ograniczone (o kilka możliwości, np. pułapki SNMP czy monitoring baz danych poprzez ODBC) środowisko Zabbix w jednym z pięciu regionów na całym świecie. Sposób utrzymania tego systemu jest identyczny jak w przypadku systemów *on-premise*, natomiast brak dostępu do serwera z poziomu systemu operacyjnego powoduje, że model ten może nie sprawdzić się w pełni w środowisku klasy *enterprise*.

Kup książkę Poleć książkę


PROGRAM
PARTNERSKI
GRUPY HELION
1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ
Zmień swoją stronę WWW w działający bankomat!
Dowiedz się więcej i dołącz już dzisiaj!
http://program-partnerski.helion.pl
GRUPA
Helion

## Czy Twoja sieć jest bezpieczna?

Cechą dzisiejszego rynku IT jest ciągła zmiana. Zmieniają się urządzenia, modyfikacjom podlega również software. Jedną z przyczyn wprowadzania kolejnych unowocześnień jest dążenie do utrzymania odpowiedniego poziomu świadczenia usług biznesowych i wysokiego poziomu bezpieczeństwa. Służy temu na przykład zastosowanie monitoringu infrastruktury, czyli użycie odpowiednich narzędzi weryfikujących stan sieci, serwerów czy też aplikacji.

Wśród rozwiązań służących monitorowaniu infrastruktury IT wyróżnia się Zabbix. Jest to platforma klasy korporacyjnej pozwalająca zbierać, przetwarzać i analizować dane, a następnie powiadamiać o problemach pochodzących z serwerów, urządzeń sieciowych i aplikacji. Oprogramowanie Zabbix jest uniwersalne i — co istotne — darmowe, a także w pełni przetłumaczone na język polski. Dzięki temu pozostaje dostępne nie tylko dla wielkich korporacji, ale również dla małych firm, które chcą zadbać o bezpieczeństwo swoich urządzeń i sieci.

## Sięgnij po książkę i poznaj:

- **komponenty oprogramowania Zabbix 7.0**
- **dobre praktyki w zakresie przygotowania środowiska jego pracy**
- **ważne aspekty związane z uruchomieniem monitoringu**
- **procesy zachodzące wewnątrz aplikacji**

Helion

helion.pl

HELION S.A.
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl

KOD KORZYŚCI
*Sięgnij po więcej!*

ISBN 978-83-289-2060-6

Cena: 69,00 zł

## Mateusz Dampc

Jest ekspertem w dziedzinie monitoringu Zabbix, posiada tytuł certyfikowanego trenera w wersjach 6.0 i 7.0. Na co dzień wspiera swoją wiedzą polską społeczność IT na forach internetowych, w ramach szkoleń, publicznych prelekcji i webinarów. W pracy skupia się głównie na realizacji ekstremalnych wymogów dotyczących monitoringu u klientów zewnętrznych. Dzięki długiemu stażowi u certyfikowanego premium partnera Zabbix na polskim rynku (Aplitt sp. z o.o.) posiada doświadczenie w zakresie Zabbix od wersji 2.2, a także certyfikaty Zabbix Certified Professional dla wszystkich wersji począwszy od 3.0.

Więcej o autorze:
*https://pl.linkedin.com/in/mateusz-dampc*

patronat:

APLITT
HUMAN FACE OF IT