Rok akademicki 2015/2016

Politechnika Warszawska

Wydział Elektroniki i Technik Informacyjnych

Instytut Informatyki



praca dyplomowa INżynierska

Mikołaj Kamiński

Monitorowanie systemów Microsoft Windows przy wykorzystaniu systemu Icinga 2

Opiekun pracy

dr inż. Piotr Gawkowski

Ocena:

Podpis Przewodniczącego

Komisji Egzaminu Dyplomowego

Kierunek: Informatyka

Specjalność: Inżynieria Systemów Informatycznych

Data urodzenia: 199308.04

Data rozpoczęcia studiów: 2012.10.01

Życiorys

Podpis studenta

EGZAMIN DYPLOMOWY

Złożył egzamin dyplomowy w dniu 20\_\_ r

z wynikiem Ogólny wynik studiów:

Dodatkowe wnioski i uwagi Komisji:

STRESZCZENIE

Streszczenie pracy w języku polskim.

Słowa kluczowe:

THESIS TITLE IN ENGLISH

Summary in English.

Keywords:

**Spis treści**

[1 Wprowadzenie 5](#_Toc438561887)

[2 Icinga 6](#_Toc438561888)

[Bibliografia 7](#_Toc438561889)

# Wprowadzenie

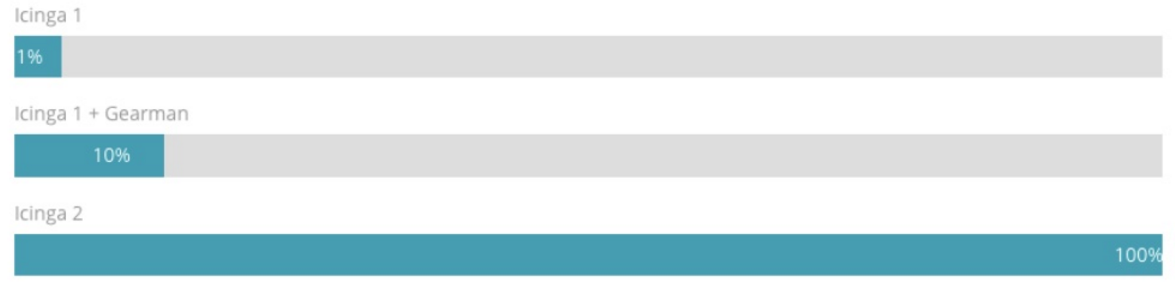
# Icinga

System monitorujący Icinga powstał w 2009 r. jak klon (ang. fork) systemu Nagios. W przeciwieństwie do protoplasty, którego bardziej zaawansowane możliwości były dostępne tylko w wersji płatnej, Icinga jest aplikacją o w pełni otwartym kodzie źródłowym, wydanym na licencji GPL[[1]](#footnote-1) wersji 2. Celem stworzenia nowego oprogramowania było nie tylko poprawienie wad oryginału, ale także dodanie nowych funkcjonalności. Należała do nich większa liczba wspieranych baz danych, a także nowy interfejs graficzny zaprojektowany i napisany w stylu Web 2.0[[2]](#footnote-2). Jednak główna koncepcja monitorowania pozostała zachowana, a twórcy oprogramowania zapewnili kompatybilność z wtyczkami przeznaczonymi do Nagiosa. Zapewniło to możliwość monitorowania wielu urządzeń i usług od początku działania systemu. Ponadto Icinga nie jest systemem wyłącznie dostępnościowym, tzn. zorientowanym na ciągłe sprawdzanie stanu infrastruktury informatycznej, ale posiada także cechy systemu analitycznego. Podstawowe zadania stawiane przed systemem Icinga to:

- sprawdzanie dostępności zasobów,

- informowanie użytkowników o awarii,

- zapewnienie obszernych danych analitycznych (ang. business intelligence data).

Dalszy rozwój tego oprogramowania oraz doprowadzenie doprowadził do wydania Icingi 2 w 2014 roku. Jednym z głównych założeń było stworzenie systemu skalowalnego oraz pozwalającego na proste rozszerzanie. Wersja 2.0 wprowadziła wiele nowych funkcjonalności oraz zmian architektonicznych, które znacznie zwiększyły wydajność systemu, co przedstawione zostało na rysunku nr 1.

**Rys. 2.1** Proporcjonalna liczba sprawdzeń, po których opóźnienie systemu wyniesie 60s. [1]

W tym rozdziale zostały zaprezentowane podstawowe informacje o systemie Icinga 2 oraz zmiany, które ten system wprowadził. Pierwsza część poświęcona jest architekturze oprogramowania. Następnie przedstawiono sposoby, w jaki może być monitorowana infrastruktura komputerowa, a także opisano konfigurację, która w nowej wersji została znacząco zmieniona.

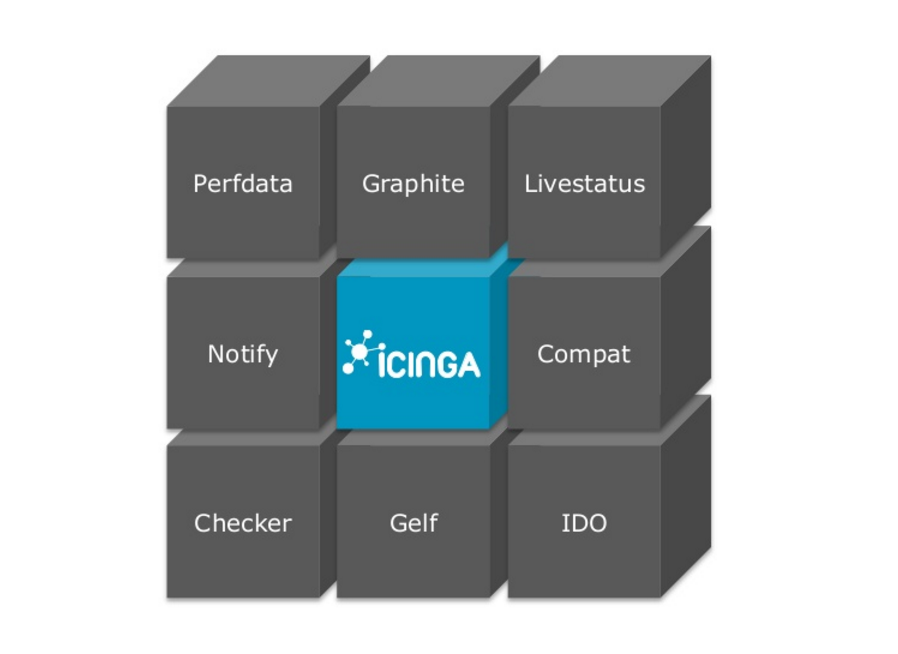
## Architektura systemu Icinga 2

System Icinga 2 składa się z dwóch głównych komponentów: rdzenia monitorującego nazywanego Icinga 2 oraz interfejsu graficznego Icinga Web 2. Osoby odpowiadające za tworzenie tego oprogramowania, wielokrotnie podkreślają [2], że ich celem jest zapewnienie jak największej możliwości integracji z innymi aplikacjami zarówno darmowymi jak i komercyjnymi. Stąd, cechą charakterystyczną obu komponentów jest modułowa budowa pozwalająca na ich proste rozszerzanie.

### Rdzeń

Rdzeń Icinga 2 został napisany w języku C++ z wykorzystaniem zbioru bibliotek Boost. Biblioteki te w znacznym stopniu rozszerzają funkcjonalność języka C++ oraz dają programiście możliwość stosowania bardziej zaawansowanych rozwiązań. Największą wadą tego zestawu jest jednak konieczność zastosowania specjalnego kompilatora oraz długi czas kompilacji programów. Boost pozwala między innymi na tworzenie i zarządzanie wątkami, które stanowią ważny element nowego rdzenia. W poprzedniej wersji monitorowanie odbywało się w jednej pętli programu, co mocno rzutowało na jego wydajność. Od wersji 2 zastosowano wielowątkowość oraz automatyczne rozdysponowanie pracy między wątkami. Dzięki temu, a także innym usprawnieniom, Icinga 2 pozwala na efektywniejszą pracę, co zostało przedstawione na rysunku 2.1.

Rdzeń początkowo był przeznaczony do działania wyłącznie na systemach linuxowych, jednak od listopada 2014 r. , kiedy to została wydana wersja 2.2, aplikacja może być również uruchamiana na systemach operacyjnych Windows oraz iOS. Umożliwiło to tworzenie tzw. klastrów monitorujących, które zostały opisane w dalszej części tego rozdziału.



**Rys. 2.2** Moduły wchodzące w skład systemu Icinga 2.

Jak zostało zaznaczone wcześniej, proste rozbudowywanie programu ma zapewniać modułowa budowa. Na rysunku 2.2 zostały przedstawione najważniejsze elementy rdzenia:

* compat – prowadzenie dziennika zdarzeń;
* IDO (Icinga Data Out) – eksport konfiguracji oraz stanu usług do bazy danych, współpracuje z bazami MySQL oraz PostgreSQL;
* gelf – integracja z systemem Graylog, służącym do zbierania i analizowania danych;
* checker – przeprowadzanie sprawdzeń stanu usług;
* notify – wysyłanie powiadomień do użytkowników;
* perfdata – zapisywanie danych wydajnościowych do plików;
* graphite – wysyłanie danych wydajnościowych przez gniazda TCP;
* livestatus – odczytywanie stanu urządzeń i usług z plików „ .dat ”.

Jak widać na powyższych opisach, część modułów ma podobne zastosowania. To, które z nich będą aktywne, zależy od budowy oraz przeznaczenia systemu i jest ustalane przez użytkownika. Zarządzanie modułami umożliwia CLI[[3]](#footnote-3) dostarczone przez system Icinga.

### Interfejs graficzny

Icinga Web, nazywana interfejsem graficznym, jest w pełni funkcjonalną i niezależną aplikacją internetową (webową). Rozwój technologii internetowych oraz urządzeń mobilnych sprawił, że konieczne się stało również ulepszenie tego elementu systemu Icinga 2. Starsza wersja była mało przyjazna zarówno dla użytkowników jak i programistów. Do szeregu wad należy zaliczyć: nieintuicyjną konfigurację w plikach XML, nadmiarową komunikację oraz skomplikowane API. Utrudniało to także integrację z innymi aplikacjami, co było jednym z głównych założeń nowego systemu.

Icinga Web 2 w części serwerowej została napisana w języku PHP przy użyciu platformy Zend Framework. Użycie takich technik programistycznych jak AJAX, umożliwiło także przesyłanie danych bez odświeżania całej strony, co zmniejszyło ilość przesyłanych danych oraz usprawniło komunikację. Ułatwieniem dla użytkowników jest przeniesienie ustawień do części graficznej oraz udostępnienie kreatora pomagającego przeprowadzić początkową konfigurację. Rozwinięte zostało także zarządzanie użytkownikami. Wprowadzono różne metody autoryzacji oraz nadawanie ról użytkownikom. Umożliwia to ograniczanie dostępu do monitorowanych urządzeń i serwisów, a także nadawanie uprawnień do korzystania z różnych modułów, wykonywania komend rdzenia Icingi czy modyfikowania konfiguracji. Kolejnym ważnym aspektem z punktu widzenia użytkownika, jest możliwość korzystania z interfejsu także na urządzeniach mobilnych, takich jak smartfony i tablety. Starsza wersja była przeznaczona jedynie dla przeglądarek działających na komputerach lub laptopach. Dla urządzeń przenośnych konieczne było utrzymywania oddzielnej aplikacji mobilnej, z której zrezygnowano w systemie Icinga 2.

Podobnie jak w rdzeniu, współpracę z innymi aplikacjami ma zapewnić modułowa budowa. Twórcom zależało, aby było to maksymalnie proste, więc aby dodać własny komponent, wystarczy, aby spełniał on kilka reguł i był umieszczony w odpowiednim katalogu. Ponadto zostały zostawione dodatkowe mechanizmy pozwalające na jeszcze głębszą integrację niż tylko rozszerzanie o dodatkowe elementy. W wielu miejscach programu zostały umieszczone tzw. zaczepy (ang. hook). Dzięki nim można dodawać własne funkcjonalności lub kod HTML bez ingerencji w kod źródłowy aplikacji. Innym sposobem modyfikowania interfejsu jest możliwość umieszczania własnych łączy internetowych. Konfigurowane może być to dla każdego z monitorowanych urządzeń lub serwisów z poziomu rdzenia (atrybut action\_url).

### Przepływ danych w systemie Icinga

Na rysunku 2.3 został przedstawiony przepływ danych w podstawowej konfiguracji systemu Icinga 2. Wyniki sprawdzeń trafiające do rdzenia przekazywane są do bazy danych przez moduł IDO, który pozwala na współpracę z bazami MySQL oraz PostgreSQL. Icinga Web 2 prezentowane dane odczytuje bezpośrednio z bazy danych. Komunikacja z rdzeniem wykorzystywana jest wyłącznie do przesyłania żądań wykonania komend udostępnianych przez rdzeń Icinga 2. Służy do tego plik komend zewnętrznych, który w rzeczywistości jest potokiem nazwanym. Jest to mechanizm służący do komunikacji między procesami w systemach UNIX, co oznacza, że oba komponenty muszą być uruchomione na tym samym urządzeniu. Wśród udostępnianych komend są też takie, które pozwalają na przetwarzanie wyników monitorowania pasywnego, co zostało opisane w następnej części rozdziału. Dodatkowo część danych, tzw. dane wydajnościowe (ang. performance data), trafia do modułów Perfmon lub Graphite. Dane te służą następnie zewnętrznym programom graficznym do generacji wykresów.

## Monitorowanie

# Bibliografia

[1] docs.icinga.org

[2] [www.icinga.org/resources/presentations/](http://www.icinga.org/resources/presentations/)

[3] [www.gnu.org/licenses/old-licenses/lgpl-2.0.html](http://www.gnu.org/licenses/old-licenses/lgpl-2.0.html)

[4] pl.wikipedia.org/wiki/Web\_2.0

1. ang. General Public License – licencja otwartego oprogramowania, treść znajduje się w [3]. [↑](#footnote-ref-1)
2. Web 2.0 – potoczne określenie serwisów internetowych, powstałych po 2001 r., w których działaniu podstawową rolę odgrywa treść generowana przez użytkowników danego serwisu. [4] [↑](#footnote-ref-2)
3. ang. Command Line Interface – interfejs wiersza poleceń [↑](#footnote-ref-3)