



AKADEMIA GÓRNICZO-HUTNICZA
IM. STANISŁAWA STASZICA
W KRAKOWIE

Wydział Fizyki i Informatyki Stosowanej

Praca inżynierska

Bartłomiej Mucha

kierunek studiów: informatyka stosowana

Migracja serwisów internetowych i integracja usług w środowisku kontenerów Docker

Opiekun: **dr inż. Piotr Gronek**

Kraków, styczeń 2020

Oświadczenie studenta

Uprzedzony(-a) o odpowiedzialności karnej na podstawie art. 115 ust. 1 i 2 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz. U. z 2018 r. poz. 1191 z późn. zm.): „Kto przywłaszcza sobie autorstwo albo wprowadza w błąd co do autorstwa całości lub części cudzego utworu albo artystycznego wykonania, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3. Tej samej karze podlega, kto rozpowszechnia bez podania nazwiska lub pseudonimu twórcy cudzy utwór w wersji oryginalnej albo w postaci opracowania, artystyczne wykonanie albo publicznie zniekształca taki utwór, artystyczne wykonanie, fonogram, wideogram lub nadanie.”, a także uprzedzony(-a) o odpowiedzialności dyscyplinarnej na podstawie art. 307 ust. 1 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2018 r. poz. 1668 z późn. zm.) „Student podlega odpowiedzialności dyscyplinarnej za naruszenie przepisów obowiązujących w uczelni oraz za czyn uchybiający godności studenta.”, oświadczam, że niniejszą pracę dyplomową wykonałem(-am) osobiście i samodzielnie i nie korzystałem(-am) ze źródeł innych niż wymienione w pracy.

Jednocześnie Uczelnia informuje, że zgodnie z art. 15a ww. ustawy o prawie autorskim i prawach pokrewnych Uczelnia przysługuje pierwszeństwo w opublikowaniu pracy dyplomowej studenta. Jeżeli Uczelnia nie opublikowała pracy dyplomowej w terminie 6 miesięcy od dnia jej obrony, autor może ją opublikować, chyba że praca jest częścią utworu zbiorowego. Ponadto Uczelnia jako podmiot, o którym mowa w art. 7 ust. 1 pkt 1 ustawy z dnia 20 lipca 2018 r. — Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2018 r. poz. 1668 z późn. zm.), może korzystać bez wynagrodzenia i bez konieczności uzyskania zgody autora z utworu stworzonego przez studenta w wyniku wykonywania obowiązków związanych z odbywaniem studiów, udostępniać utwór ministrowi właściwemu do spraw szkolnictwa wyższego i nauki oraz korzystać z utworów znajdujących się w prowadzonych przez niego bazach danych, w celu sprawdzania z wykorzystaniem systemu antyplagiatowego. Minister właściwy do spraw szkolnictwa wyższego i nauki może korzystać z prac dyplomowych znajdujących się w prowadzonych przez niego bazach danych w zakresie niezbędnym do zapewnienia prawidłowego utrzymania i rozwoju tych baz oraz współpracujących z nimi systemów informatycznych.

.....
(czytelny podpis)

Spis treści

1	Wstęp	5
1.1	Cel pracy	6
1.2	Założenia projektu	6
2	Podstawa Teoretyczna	8
2.1	Wirtualizacja	8
2.1.1	Poziom architektury zestawu instrukcji (ISA)	9
2.1.2	Poziom warstwy abstrakcji sprzętowej (HAL)	10
2.1.3	Poziom systemu operacyjnego	10
2.1.4	Poziom bibliotek lub języków programownia	10
2.1.5	Poziom aplikacji	10
2.2	Hipernadzorca	11
2.2.1	Hipernadzorca typu pierwszego	11
2.2.2	Hipernadzorca typu drugiego	11
2.3	Konteneryzacja	11
3	Założenia projektowe	13
3.1	Architektura wejściowa serwisów	13
3.1.1	Platforma systemu serwerowego	13
3.1.2	Wizualizacja platformy wejściowej	13
3.2	Architektura docelowa serwisów	13
4	Opis przykładowych aplikacji i ich wdrożenie	14
4.1	Opis	14
4.2	Środowisko projektowe i wymagania aplikacji	14
4.3	Działanie i powiązania zbioru konenerów	15
4.4	Zrealizowane pliki dockerfile	16
5	Wdrożenie rzeczywistych serwisów wydziałowego systemu informa- tycznego	17

<i>SPIS TREŚCI</i>	4
6 Wnioski	18
7 Kod źródłowy	19
7.1 Repozytorium Git	19
7.2 Dołączona płyta CD	19
8 Bibliografia	20

Rozdział 1

Wstęp

Możliwości jakie oferują maszyny wirtualne są nieocenione we współczesnym świecie. Systemy serwerowe w skład których mogą wchodzić nawet tysiące powiązanych ze sobą lub indywidualnych serwisów nie mogą być albo są zasadniczo trudne do wdrożenia na jednej platformie o określonym systemie operacyjnym, konfiguracji i innych elementach wchodzących w skład szerokorozumianego środowiska. Maszyny wirtualne są rozwiązaniem na to zagadnienie. Każda maszyna wirtualna może zostać stworzona niezależnie od architektury sprzętowej i oferuje dowolne środowisko, które jednocześnie będzie wyizolowane od środowisk gospodarza (host) i innych maszyn wirtualnych (guest). Korzyścią płynącą z izolacji środowiska jest chociażby zwiększone bezpieczeństwo systemu, ułatwienie zarządzania serwisami oraz wdrażania nowych wersji aplikacji. Niezadko używane są serwisy szczególnie stare, a jednak spełniające swoje zadanie, które wymagają rozwiązań już nieaktualnych wersji elementów środowiskowych, nie wspieranych przez nowsze wersje. Co za tym idzie wdrożenie np. dwóch aplikacji działających w ramach tej samej technologii, ale na innych wersjach będzie tworzyć konflikt. Problemy tego typu zanikają w kontekście wirtualizacji, albo wcale nie stoi na przeszkodzie osadzenia każdej pojedynczej aplikacji na osobnej maszynie. Wirtualizacja posiada jednak szereg wad. Taką wadą jest na przykład to, że każda maszyna wirtualna musi rezerwować określoną i niezmienną w czasie działania ilość zasobów, takich jak pamięć operacyjna, twarda oraz liczbę wątków procesora i wiele innych. Stawia to przed administratorem problem jakim jest dobranie parametrów jakimi taka maszyna ma się cechować. Przydzielnie zbyt małej ilości zasobów sprawi, że serwis będzie niedomagał. Z kolei przydzielnie zbyt dużej doprowadzi do marnowania się zasobów, które mogłyby być lepiej wykorzystane. To jak maszyna wirtualna zużywa zasoby takie jak pamięć operacyjna nie są kontrolowane, zarezerwowany zasób jest statyczny i nie jest zwalniany w przypadku braku użycia. Rozwiązaniem tego problemu jest zmiana podejścia do koncepcji wirtualizacji, a

mianowicie konteryzacja serwisów. Platformy takie jak Docker czy LXC pozwalają tworzyć nie wymagające udziału hipernadzorcy wyizolowane środowiska o dynamicznie przydzielanych zasobach, tak zwane kontenery. Ze względu na to, że kontenery zarządzane przez platformę docker współdzielą jądro systemowe z gospodarzem i innymi kontenerami, a w ramach osadzenia aplikacji wystarczy dostarczyć zbudowaną aplikację oraz wymagane do poprawnego jej działania składniki systemów można zaoszczędzić na użyciu pamięci twardej względem tej samej aplikacji wdrożonej na maszynie wirtualnej.

1.1 Cel pracy

Celem pracy jest przeniesienie aplikacji z maszyn wirtualnych na kontenery oraz opracowanie tej metodologii. W konsekwencji zostaną stworzone skalowalne środowiska usług internetowych, działające w oparciu o technologię kontenerów Docker na platformie Linux w systemie wirtualizacji VMware ESX oraz porównanie i ocena korzyści wynikających z tych działań. Modelem przykładowym jest system aplikacji działających w technologii php i java z frameworkiem springboot oraz baza danych PostgreSQL na trzech osobnych kontenerach Docker. Kontenery będą osadzone na zainstalowanej w systemie wirtualizacji ESX maszynie wirtualnej z system operacyjnym Debian 10. Finalnie wdrożone zostaną realne serwisy w wydziałowej sieci komputerowej.

Plan pracy jest następujący. W części teoretycznej zostaną omówione mechanizmy stojące za działaniem maszyn wirtualnych i kontenerów na platformie docker oraz ich porównanie. Następnie omówiony zostanie schemat wdrożenia aplikacji. Część praktyczna będzie zawierać szczegółowy opis przygotowania środowiska oraz wdrożenia aplikacji zarówno przykładowych jak i tych pochodzących z wydziałowego systemu informatycznego.

1.2 Założenia projektu

Celem projektowej części pracy jest opracowanie skalowalnego środowiska usług internetowych, działającego w oparciu o technologię kontenerów Docker na platformie Linux w systemie wirtualizacji VMware ESX. Usługi realizowane przez system mają obejmować obsługę: - internetowych serwisów aplikacyjnych działających w technologiach odpowiednio: PHP, Apache Tomcat, Python Django, - witryn CMS WordPress, - serwerów relacyjnych baz danych MySQL, PostgreSQL. Elementem pracy będzie także migracja istniejących serwisów internetowych do ich odpowia-

jących im instancji wyżej wymienionych kontenerów Docker oraz ocena uzyskanych korzyści pod kątem konsumowanych zasobów sprzętowych i wydajności działania.

Rozdział 2

Podstawa Teoretyczna

2.1 Wirtualizacja

Szeroko rozumiane urządzenie zwane komputerem składa się z dwóch kategorii komponentów: urządzeń fizycznych i oprogramowania. W skład urządzeń fizycznych wchodzi między innymi płyta główna, centralna jednostka przetwarzająca i urządzenia wejścia/wyjścia. Oprogramowanie składa się z warstw, najniżej, najbliższej sprzętu znajduje się oprogramowanie do zarządzania i komunikacji z urządzeniami, w wyższych warstwach znajdziemy aplikacje użytkowe. Zadaniem systemu operacyjnego jest zarządzanie zarówno zasobami sprzętowymi jak i oprogramowaniem. Stanowi on interfejs pomiędzy maszyną a użytkownikiem, umożliwiając tym samym stosowanie komputerów do celów osobistych znanych nam z życia codziennego i profesjonalnych na linii człowiek - maszyna, ale i maszyna - maszyna. Ideą stojącą za systemem operacyjnym jest istnienie środowiska, które dynamicznie będzie tłumaczyć zlecenia użytkownika na język maszynowy, następnie zlecać sprzętowi ich wykonanie i w drugą stronę poinformować użytkownika o rezultatach pracy maszyny oraz jej zapotrzebowaniach na dane, zachowując jednocześnie optymalne działanie pracy całego systemu i zawartych w nim urządzeń.



Rysunek 2.1: Schmat warstw systemu operacyjnego

Na powyższym rysunku 2.1 przedstawiony jest schemat budowy systemu operacyjnego. W skład samego systemu operacyjnego wchodzi sterowniki, jądro i powłoki systemowe. System operacyjny jest również podzielony na przestrzeń jądra i użytkownika. Wirtualizacja zatem jest symulacją warstwy fizycznej komputera na której można zainstalować i używać dowolnego systemu operacyjnego. Zasymulować można różnego rodzaju architektury i parametry sprzętowe, zalecane jest jednak by wirtualna platforma sprzętowa nie przekraczała możliwości rzeczywistego sprzętu. Wirtualizacji można dokonać na kilku poziomach.

2.1.1 Poziom architektury zestawu instrukcji (ISA)

Tak zwana pełna wirtualizacja. Wszystkie instrukcje procesorowe systemu gościa są interpretowane przez emulator, a następnie mapowane na rzeczywisty sprzęt fizyczny gospodarza. Dalej instrukcje są wykonywane i zwracane do emulatora który przekazuje je do gościa. Z racji długiej drogi jaką musi pokonać pojedyncza instrukcja to rozwiązanie należy do najwolniejszych. Tą metodę stosuje się, gdy architektury sprzętowe gościa i gospodarza są zbyt różne, aby dało się je zmapować lub jest to nieopłacalnie trudne. Rozwiązanie to stosuje się na przykład do emulacji środowisk smartfonów, konsol do gier i mikrokontrolerów.

2.1.2 Poziom warstwy abstrakcji sprzętowej (HAL)

Inaczej nazywany poziomem sprzętowego wspomagania. Ta metoda wirtualizacji polega na mapowaniu rzeczywistych zasobów sprzętowych na wirtualne zasoby. Zatem wszystkie instrukcje nieuprzywilejowane są wykonywane bezpośrednio na sprzęcie gospodarza. Instrukcje uprzywilejowane, czyli takie które może wykonać tylko gospodarz są przekazywane do hipernadzorcy i ten je wykonuje. Rozwiązanie to jest zasadniczo szybsze od wirtualizacji zestawu instrukcji. Z tej metody korzystają narzędzia do wirtualizacji takie jak VMWare Workstation, Oracle VirtualBox i wiele innych.

2.1.3 Poziom systemu operacyjnego

Wirtualizacja na poziomie systemu operacyjnego pozwala na działanie kilku odrębnych odizolowanych od siebie systemów operacyjnych, a dokładnie przestrzeni użytkownika korzystających z jednego jądra systemowego. Co za tym idzie nie dochodzi do duplikacji całych systemów operacyjnych i co za tym idzie nie jest wymagana praca hipernadzorcy. Rozwiązanie takie jest nazywane konteneryzacją i jest stosowane na takich platformach jak Docker, CoreOS, LXC i Oracle Solaris Containers. Wadą tej metody jest przymus używania tylko takich systemów operacyjnych, które mogą współdzielić jądro z systemem gospodarza. Nic jednak nie stoi na przeszkodzie aby umieścić kontenery na maszynie wirtualnej postawionej na poziomie wspierania sprzętowego, jednak spowolni to szybkość tych kontenerów do szybkości samej maszyny wirtualnej.

2.1.4 Poziom bibliotek lub języków programownia

Stosowane w ramach technologii JIT (just in time). Niektóre środowiska programistyczne pozwalają na kompilację kodu źródłowego do postaci kodu pośredniego, który nie ma bezpośredniego przełożenia na kod maszynowy. Program jest wykonywany na maszynie wirtualnej, która kompiluje kod pośredni do kodu maszynowego, a może to zrobić zarówno na początku wywołania programu lub pierwszego wywołania konkretnej części kodu. Z tej technologii korzysta Java, .Net, Python i wiele innych języków programowania.

2.1.5 Poziom aplikacji

Wirtualizowane są tylko aplikacje, co oznacza, że nie wykorzystują one bezpośrednio dostarczanego przez system operacyjny środowiska wykonawczego, a używają

dostarczonego przez inną aplikację takie środowisko na jakie zostały zbudowane. Przykładem platformy umożliwiającej wirtualizację aplikacji jest Wine, która umożliwia działanie aplikacji przystosowanych do pracy w systemie MS Windows na systemie operacyjnym typu Linux.

2.2 Hipernadzorca

Komponentem systemu komputerowego umożliwiającym dokonanie wirtualizacji na poziomie wsparcia sprzętowego jest hipernadzorca (hypervisor). Rozróżniamy dwa typy hipernadzorców:

2.2.1 Hipernadzorca typu pierwszego

Tak zwany hipernadzorca natywny (bare metal) osadzony bezpośrednio na sprzęcie nie wymaga zainstalowanego systemu operacyjnego gospodarza. Pozwala on osadzać maszyny wirtualne nad sobą co znacząco upraszcza schemat abstrakcji architektury całego systemu. Przykładami tego typu hipernadzorców są MS Hyper-V i VMWare ESXi.

2.2.2 Hipernadzorca typu drugiego

Hipernadzorca hostowany jest osadzony w systemie operacyjnym gospodarza jako aplikacja. Takimi aplikacjami są przykładowo VMWare Workstation, VMWare Player, VirtualBox i QEMU.

2.3 Konteneryzacja

Konteneryzacja jako wirtualizacja na poziomie systemu operacyjnego z racji współdzielenia przez kontenery jądra systemu gospodarza powinna cechować większą wydajnością od wirtualizacji na poziomie ISA lub HAL. O ile nie zastąpi ona klasycznych maszyn wirtualnych pod względem możliwości uruchamiania różnorodnych systemów operacyjnych, a tyle najmocniejszą stroną konteneryzacji jest dużo niższe zapotrzebowanie na pamięć twardą, co za tym idzie przenaszalność oraz szybkość zarówno działania jak i startowania. Współdzielenie jądra systemowego oraz dostępu do fizycznej warstwy komputera niesie ze sobą pewne ryzyko jakim jest drastyczny spadek wydajności. Wszystkie kontenery konkurują ze sobą o zasoby sprzętowe, ale również o zasoby jądra. Jądro systemu jest bardzo skomplikowanym oprogramowaniem. Zdaża się, że zbyt obciążone przez kontenery jądro znacząco spowolni, a w konsekwencji

utworzy szyjkę od butelki (bottle neck) pomiędzy warstwami użytkownika i warstwą fizyczną.

Rozdział 3

Założenia projektowe

3.1 Architektura wejściowa serwisów

3.1.1 Platforma systemu serwerowego

Na wydziałowym serwerze zainstalowany jest hipernadzorca typu pierwszego, dokładnie VMWare ESX, osadzony bezpośrednio nad warstwą fizyczną klastra komputerowego. Na serwerze wdrożonych jest szereg aplikacji działających na odrębnych maszynach wirtualnych.

3.1.2 Wizualizacja platformy wejściowej

Na poniższym rysunku znajduje się schemat wejściowej architektury systemu serwerowego, który w ramach tej pracy ma zostać przekształcony.

3.2 Architektura docelowa serwisów

Koncepcja architektury docelowej jest zlikwidowanie pewnej ilości maszyn wirtualnych i przeniesienie serwisów w nich zawartych do kontenerów znajdujących się w jednej maszynie wirtualnej. Oczywiście korzyścią z tej akcji jest zaoszczędzenie pewnej, być może nawet dużej ilości pamięci twardej. Nie jest jednak oczywiste do jakiej zmiany dojdzie w kwestii wydajności. O ile pierwotny układ składa się z jednego poziomu wirtualizacji, tak ten układ będzie się składał z dwóch: wirtualizacji wspomaganej sprzętowo oraz na poziomie systemu oparcyjnego.

Rozdział 4

Opis przykładowych aplikacji i ich wdrożenie

4.1 Opis

Przykładowe aplikacje to najprostsze aplikację o identycznych wymaganiach jak aplikację pochodzące z wydziałwego serwera. Aplikacja java spring boot jest najprostszym serwisem http wyświetlający prostą zawartość w przeglądarce internetowej. Serwis apache-php również jest serwisem http, który udostępnia przez przeglądarkę interfejs CRUD do trzeciego serwisu, który dostarcza bazę danych PostgreSQL.

4.2 Środowisko projektowe i wymagania aplikacji

Środowisko projektowe:

- Narzędzie do wirtualizacji VMWare Workstation Player 15.5
- System operacyjny Debian 10.2
- Docker 19.03.5
- Docker-compose 1.25.0

Wymagania Aplikacji:

- Aplikacja Java Spring Boot
 - ★ Java 8 lub nowsza
- Aplikacja php
 - ★ php 5.4 lub nowsze z dodatkiem umożliwiającym połączenie z bazą danych PostgreSQL

- ★ Apache 2 lub nowszy
- ★ Dostęp do istniejącej bazy danych PostgreSQL

4.3 Działanie i powiązania zbioru konenerów

Docker

Platforma Docker do utworzenia kontenera wymaga dwóch komponentów zbudowanej aplikacji i jej zasobów w postaci na przykład plików html, skryptów itd. oraz pliku konfiguracyjnego dockerfile na podstawie którego zostanie utworzona przestrzeń użytkownika w kontenerze. Wykorzystanymi komendami dockerfile w projekcie są:

- RUN wykonuje polecenie powłoki systemu operacyjnego w konenerze podczas jego budowy
- CMD nadpisuje domyślną instrukcję 'command', która domyślnie uruchamia aplikację wewnątrz kontenera. Dotyczy to przypadku w którym kontener pracuje w trybie odłączonym od powłoki systemu gospodarza. Instrukcja CMD może zostać wykorzystana raz, każda kolejna nadpisze poprzednią, w konsekwencji wykonana zostanie tylko ostatnia.
- COPY kopiuje pod podane miejsce w systemie plików gościa wskazane pliki i katalogi z systemu plików gospodarza
- ADD jest to rozszerzona instrukcja COPY, pozwala również dodać plików z podanego adresu url oraz automatycznie rozpakować foldery skompresowane w trakcie kopiowania
- ENTRYPOINT wykonuje tę samą czynność co CMD z tą różnicą, że może być użyta wielokrotnie i każde użycie zostanie wykonane. Instrukcje ENTRYPOINT i CMD nie kolidują ze sobą
- VOLUME tworzy obszar w pamięci w którym będzie przechowywana kopia danych wygenerowanych przez kontener, np. logi, bazy danych itd.
- FROM instrukcja której obecność jest zawsze wymagana do zbudowania obrazu. Musi znajdować się w pierwszej linii pliku docker file. Jej argumentem jest tag obrazu który ma zostać zbudowany. W trakcie budowy obraz jest pobierany z repozytorium.
- ENV tworzy zmienną środowiskową w goszczonym systemie operacyjnym
- EXPOSE pokazuje port widoczny dla maszyn zewnętrznych

Z racji tego, iż wybranym system operacyjnym gospodarza dla kontenerów jest Debian 10, dockerfile musi zawierać komendy która zainstaluje wymagane do działania

aplikacji paczki i biblioteki oraz koniecznie korzystać z obrazów systemów z rodziny Linux. Musi również zawierać

Docker-compose

W przypadku kiedy w systemie pracuje wiele kontenerów pojawia się problem zarządzania nimi. Uruchamianie każdego kontenera z wiersza poleceń jest żmudnym i podatnym na pomyłki procesem. Zastosowanie skryptu np. w powłoce bash cechowałoby się nie małą nieprzerzystością. Programem służącym do tego celu jest Docker-compose. Pozwala on budowanie i uruchamianie wielu kontenerów docker jednocześnie. Tak jak Docker, Docker-compose wymaga pliku konfiguracyjnego, tym razem w notacji YAML i o rozszerzeniu docker-compose.yml. W tym pliku są zawarte lokalacje plików dockerfile i parametry służące do budowy i uruchomienia obrazu oraz konfiguracja sterowników np. sieciowych.

Aplikacja Java spring boot

Realizuje najprostsze zadanie. Wyświetla "Hell World!"

Aplikacja php

Baza danych PostgreSQL

4.4 Zrealizowane pliki dockerfile

Rozdział 5

Wdrożenie rzeczywistych serwisów wydziałowego systemu informatycznego

Rozdział 6

Wnioski

Rozdział 7

Kod źródłowy

7.1 Repozytorium Git

7.2 Dołączona płyta CD

Rozdział 8

Bibliografia