AMAZON WEB SERVICES

Podstawy korzystania z chmury AWS

Helion

Tytuł oryginału: Learning Amazon Web Services (AWS): A Hands-On Guide to the Fundamentals of AWS Cloud

Tłumaczenie: Joanna Zatorska

ISBN: 978-83-283-6474-5

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 231 22 19, 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *http://helion.pl* (księgarnia internetowa, katalog książek)

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

Printed in Poland.

Spis treści

1

Poznajemy AWS

O książce

Papierowe wydanie książki wraz z załączoną biblioteką filmów wideo koncentruje się na chmurze usług AWS (*Amazon Web Services*), a szczególnie na modelu *IaaS* (*Infrastructure as a Service* — infrastruktura jako usługa). Z pomocą tej książki czytelnicy z łatwością nauczą się korzystać z usług w chmurze oferowanych przez Amazon. Wspomniane usługi można podzielić na podstawowe usługi obliczeniowe, magazynowe, sieciowe oraz zabezpieczeń, a także znacznie ułatwiające automatyzację. AWS warto traktować jak ogromną skrzynkę narzędziową, wypełnioną różnorodnymi wyspecjalizowanymi narzędziami, przy użyciu których można wykonać wiele zadań związanych z infrastrukturą. W książce opisałem podstawy techniczne usług AWS, które docenią administratorzy systemów, programiści lub kierownicy projektów oraz inni, którzy słyszeli o chmurze AWS i chcieliby poszerzyć swoją wiedzę. W książce tej wyjaśniłem najważniejsze koncepcje, niektóre z najważniejszych komponentów oraz sposób przygotowania usług do poprawnego działania poprzez odpowiednią konfigurację. Podczas pracy nad książką przejrzałem ponad 35 000 stron dokumentacji i na podstawie informacji o aspektach technicznych AWS napisałem podsumowanie o objętości 300 – 400 stron. Nie twierdzę, że po przeczytaniu tej książki nie będzie trzeba już zaglądać do dokumentacji AWS. Na pewno okaże się to konieczne; mam jednak nadzieję, że książka oraz dołączona do niej biblioteka filmów wideo pozwolą na szybki podbój dżungli AWS.

Niektórzy zapewne będą chcieli uzyskać certyfikat; jednak książka nie koncentruje się bezpośrednio na certyfikacji AWS. Jej celem jest omówienie fundamentalnych usług. Wszystkie testy przeprowadzane podczas certyfikacji AWS koncentrują się na rozwiązywaniu problemów dotyczących konkretnych scenariuszy. Kandydat musi wybrać jedną lub dwie najlepsze odpowiedzi; znajomość fundamentalnych usług jest przy tym niezbędna. Jeśli ktoś chce uzyskać certyfikat związany z usługami w chmurze AWS, a szczególnie z architekturą AWS, musi na wylot poznać fundamentalne usługi AWS. Musi też poświęcić kilka godzin na praktyczną pracę z usługami AWS. Jeśli ktoś chce tworzyć aplikacje hostowane na AWS, musi jeszcze dokładniej poznać fundamentalne usługi. Nie należy się

też łudzić, że przeczytanie jednej książki wystarczy; jest to niemożliwe, zwłaszcza że AWS ciągle się zmienia. Wyjaśniam, jak sobie z tym poradzić.

Każdy rozdział tej książki dotyczy konkretnej koncepcji lub usługi AWS i zawiera solidny, szczegółowy opis techniczny. Nie ma tu jednak stron wypełnionych instrukcjami krok po kroku, ponieważ poszczególne czynności zmieniają się co kilka miesięcy. Podczas pisania tej książki trzykrotnie zmieniono wygląd ikon wykorzystywanych w dokumentacji technicznej AWS. Dodano też 600 funkcji oraz wprowadzono wiele innych zmian. Niektóre z nich były kosmetyczne, a inne dość znaczące.

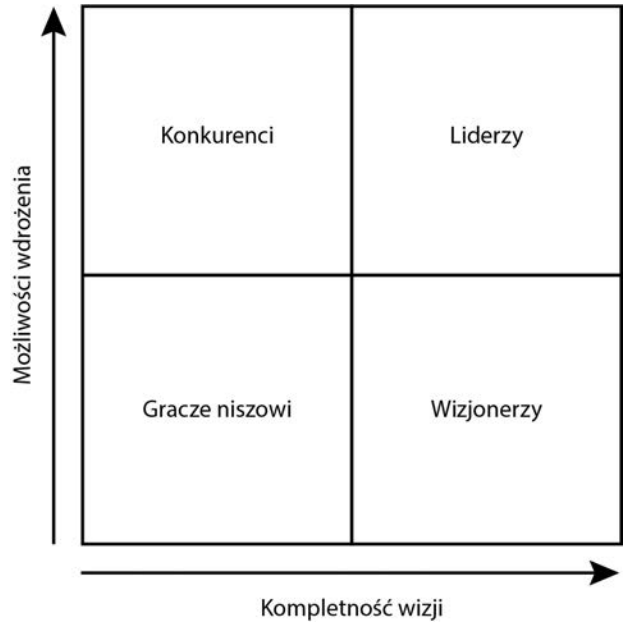
Aby zaradzić szybkiej dezaktualizacji, do książki dołączono zbiór filmów, prezentujących konfigurację i instalowanie wielu usług w chmurze AWS. Filmy te są dostępne pod adresem *ftp://ftp.helion.pl/przyklady/amwese.zip*.

W poszczególnych rozdziałach zachęcam do obejrzenia filmów dotyczących poruszanej tematyki. Filmy zawierające instrukcje krok po kroku można modyfikować, aktualizować lub dodawać, w zależności od zmian w usługach AWS. Zaletą filmów wideo jest możliwość ich wstrzymania oraz przewijania w trakcie nauki. Ruszajmy zatem w podróż i sprawdźmy, dokąd dotrzemy. Oto zagadnienia przedstawione w pierwszym rozdziale.

- Definicja chmury publicznej
- Jak AWS spełnia warunki metodologii IaaS oraz platforma jako usługa (PaaS)
- Cechy chmury obliczeniowej według NIST
- Co należy uwzględnić przed migracją aplikacji do AWS
- Korzyści operacyjne wynikające z korzystania z chmury
- Umowa o gwarantowanym poziomie świadczenia usług w chmurze (SLA)
- Bezpieczeństwo danych, aplikacji oraz sieci w AWS
- Zagadnienia zgodności w AWS
- AWS jako platforma o dobrze zaprojektowanej architekturze

Próba zdefiniowania chmury

Publiczna chmura obliczeniowa nie jest niczym nowym; dostawcy chmur publicznych Amazon Web Services i Microsoft Azure prowadzą działalność już ponad dekadę, oferując usługi IaaS oraz PaaS na całym świecie. Innymi wartymi uwagi rozwiązaniami są Google Cloud Platform (GCP), IBM oraz Oracle Cloud. Magiczny kwadrat Gartnera (*www.gartner.com/en/research/methodologies/magic-quadrants-research*), przedstawiony na rysunku 1.1, obrazuje cztery rodzaje dostawców technologii, do których firma może dostosować swoje cele i strategie. W roku 2018 rynek IaaS zdominował dwie z tych kategorii. W obszarze Liderzy dominowały usługi Amazon Web Services. Tuż za nimi uplasowały się rozwiązania firmy Microsoft, a następnie Google. Firma Google znalazła się też blisko obszaru Wizjonerów. Alibaba Cloud, Oracle i IBM znalazły ostoję w obszarze Graczy Niszowych.



Rysunek 1.1. Najważniejsi dostawcy chmury publicznej. Gartner, Magic Quadrant for Cloud Infrastructure as a Service, Worldwide, Dennis Smith et al., 23 May 2018. (Gartner Methodologies, Magic Quadrant, www.gartner.com/en/research/methodologies/magic-quadrants-research)[1]

Gdy zaczynałem karierę jako technik komputerowy w latach 90. ubiegłego wieku, większość korporacji, w których pracowałem, korzystała z różnych usług komputerowych znajdujących się poza siedzibą firmy. Usługi księgowe były dostępne poprzez szybkie (jak na tamte czasy) połączenia modemowe o prędkości 1200 bitów na sekundę, obsługiwane przez terminale cyfrowe z zielonymi wyświetlaczami. Kabel szeregowy biegnący z sufitu do terminala był tak solidny, że mógłby posłużyć do holowania samochodu.

Jeden z moich ówczesnych klientów korzystał z księgowości za pośrednictwem komputera typu mainframe zlokalizowanego w jego miejscowości. Nie miał jednak dostępu do usług księgowych w dowolnym czasie; miał jedynie do dyspozycji wyznaczony czas w każdy wtorek. Płatności z kolei obsługiwała inna usługa zdalna o nazwie Automatic Data Processing, w skrócie ADP. Usługi te, a także dostarczające je firmy, są nadal obecne na rynku. IBM nadal wydaje kolejne wersje serwerów mainframe Z, a firma ADP oferująca usługi płatnicze była jedną z pierwszych firm sprzedających oprogramowanie jako usługę (SaaS), która nadal cieszy się popularnością.

[1] Gartner w swoich publikacjach nie wymienia żadnego dostawcy, produktu ani usługi, a także nie sugeruje użytkownikom korzystania z technologii dostarczanych tylko przez dostawców z najwyższych pozycji rankingu. Publikacje badawcze firmy Gartner zawierają jej opinie i nie należy ich traktować jako stwierdzenia faktów. Gartner nie udziela jakichkolwiek gwarancji, wyraźnych bądź dorozumianych, dotyczących tej publikacji, włącznie z gwarancjami zbytu oraz przydatności do określonego celu.

W roku 2015 firma IBM kupiła dostawcę usług w chmurze z Teksasu, firmę SoftLayer i dołączyła jej produkty do swojej oferty chmury publicznej, zwanej obecnie IBM Cloud. Serwery mainframe Z zaczęto hostować w chmurze IBM, zapewniając hostowane usługi mainframe; w kwietniu roku 2018 firma IBM ogłosiła uruchomienie tak zwanych „cienkich serwerów mainframe" dla chmury obliczeniowej, opartych na serwerach z14.

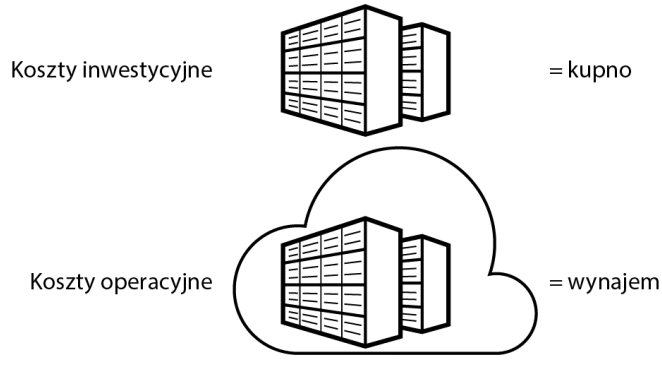
Usługi obliczeniowe w bankach i instytucjach finansowych prawdopodobnie w 50% opierają się na serwerach mainframe firmy IBM. Jest to świetna wiadomość dla firm, które nie chcą utrzymywać lokalnego środowiska typu mainframe.

Pięćdziesiąt lat po uruchomieniu serwerów mainframe przez IBM technologie tego typu oferowane przez inne firmy są nadal wykorzystywane i wchodzą w skład krajobrazu chmury publicznej.

W rzeczywistości ponad 90 ze 100 największych banków na świecie, 10 największych firm ubezpieczeniowych, większość z 25 największych sprzedawców i większość z największych na świecie linii lotniczych nadal wykorzystuje serwery mainframe firmy IBM.

Jeśli nawet ktoś nie korzystał jeszcze z serwerów mainframe, prawdopodobnie zetknął się z cyklem wdrażania NetWare firmy Novell, Windows i Active Directory, a także z wirtualizacją z wykorzystaniem VMware lub Hyper-V. Prawdopodobnie korzysta z chmury prywatnej w swoich centrach danych i może się zastanawia, dlaczego jego firma przenosi się do chmury publicznej.

Tworzenie i utrzymanie centrów danych jest kosztowne. Zbudowanie centrum danych kosztuje kilka milionów lub miliardów dolarów. Utrzymanie istniejącego centrum danych przez dłuższy czas także jest kosztowne. Ze względu na wirtualizację oraz wzrost znaczenia internetu jako przydatnego medium komunikacyjnego, usługi w chmurze zastąpiły i będą zastępować wiele lokalnych centrów danych. Koszty inwestycyjne ponoszone podczas hostowania aplikacji w chmurze publicznej, zastępujące koszty utrzymywania ich we własnym centrum danych, niekiedy określa się jako koszt wynajmu zamiast kupna, zgodnie z rysunkiem 1.2.



Rysunek 1.2. Brak długotrwałych kosztów inwestycyjnych

Podczas korzystania z usług w chmurze ponosi się tylko koszty operacyjne. Nakłady inwestycyjne niezbędne do utworzenia centrum danych nie muszą obciążać jednej firmy.

Wydatki operacyjne są jednak nadal wysokie. Możemy oznajmić szefowi, że „nie potrzebujemy 800 milionów dolarów na utworzenie centrum danych, ale każdego roku będziemy musieli wydać 2 miliony dolarów".

Prawdą jest, że po podliczeniu wszystkich wydatków koszt utrzymania i hostowania aplikacji w chmurze jest niższy. Jednak działalność w chmurze będzie tańsza, tylko jeśli hostowane w chmurze usługi zostaną poprawnie zaprojektowane. Usługi i aplikacje nie działają przez 24 godziny 7 dni w tygodniu; gdy nie są potrzebne, wyłącza się je lub zmniejsza skalę działania. Nie wszyscy znają koncepcję automatyzacji. Dostawcy usług w chmurze publicznej korzystają z automatycznych procedur budowania, monitorowania i skalowania każdej usługi w chmurze oraz zarządzania nią. Jeszcze przed ukończeniem czytania tej książki będzie jasne, że automatyzacja jest sekretnym składnikiem udanego wdrożenia każdej usługi w chmurze. Dzięki zautomatyzowanym procedurom uda się zaoszczędzić pieniądze i zapewnić sobie spokojny sen.

Zacznę od zdefiniowania chmury publicznej. Chmura jest po prostu kolekcją centrów danych. Z punktu widzenia klienta nie ma mowy o własności; właścicielem usług jest dostawca chmury, a klient może wynająć każdą usługę. Niektórzy sądzą, że chmura opiera się tylko na zasobach wirtualnych, ale chmura AWS *może* zaoferować fizyczne serwery. Jeśli zechcemy, Amazon umożliwi hosting aplikacji i baz danych na fizycznych serwerach znajdujących się w centrach danych tej firmy. Oczywiście zwykle korzysta się z oferty AWS zapewniającej serwery wirtualne w ponad 150 różnych rozmiarach i konfiguracjach. Amazon może też umożliwić wykorzystywanie własnych lokalnych centrów danych we współpracy z zasobami i usługami w chmurze AWS. Jak widać, trudno współcześnie definiować chmurę inaczej niż jako ogromny zbiór sieciowych zasobów obliczeniowych i magazynowych, hostowanych w centrach danych dostępnych przez internet lub z wykorzystaniem połączeń prywatnych.

Wszystko, co hostujemy w chmurze publicznej, wykorzystuje zasoby obliczeniowe i magazynowe do obsługi aplikacji. Natomiast wszystkie urządzenia fizyczne, takie jak routery, switche i macierze dyskowe, można zastąpić oprogramowaniem od zewnętrznych dostawców lub usługą programistyczną zarządzaną przez AWS, wykorzystującą wirtualne komputery, magazyn oraz komponenty sieciowe. Nie oznacza to, że wiele firm nie korzysta już z urządzeń fizycznych. Urządzenia fizyczne, takie jak routery i switche, cechują się niesamowitą szybkością i najczęściej mogą działać znacznie szybciej od ich programistycznych odpowiedników. Co się jednak stanie, jeśli będziemy mieć do dyspozycji setki lub tysiące wirtualnych maszyn wykonujących równolegle funkcje switcha lub routera sprzętowego? Być może nie będziemy już potrzebować żadnego urządzenia sieciowego. Większość usług w chmurze zarządzanych przez AWS jest hostowana na maszynach wirtualnych (określanych mianem instancji EC2 lub Elastic Cloud Compute), z ogromnymi zasobami procesorów i pamięci RAM, uruchomionych na wielkich farmach serwerów ze specjalnie opracowanymi aplikacjami. Zapewniają one macierze dyskowe, usługi sieciowe, równoważenie obciążenia oraz automatyczne skalowanie, z których korzystamy w ramach AWS.

Przenoszenie się do AWS

Gdy zapadnie decyzja o przenosinach do chmury AWS, wprawiamy w ruch machinę złożoną z niezliczonych elementów. Należy wyszkolić pracowników, wprowadzić zmiany w architekturze, zmienić nawyki programistów, a także przyspieszyć decyzję specjalistów ds. IT dotyczącą wyboru dostawcy usług w chmurze; nie ma czasu do stracenia. Większe firmy często próbują przekonać pracowników, jak wielkie znaczenie mają przenosiny do chmury. Często kierownictwo firmy ma na ten temat zdecydowaną opinię. Niestety, nie zawsze opiera się ona na wiedzy technicznej czy na praktycznym doświadczeniu z wybranym dostawcą usług w chmurze. Ogólnie rzecz biorąc, w firmach korzystających z takich usług zwykle dominuje jeden z następujących sposobów myślenia.

- **Myślenie korporacyjne**. Obecnie firma dysponuje centrami danych, infrastrukturą i zwirtualizowanymi aplikacjami. Stale rosnące koszty infrastruktury i utrzymania sprawiają, że zaczyna się przyglądać możliwościom chmury publicznej.
- **Myślenie urodzonego w chmurze**. Jest charakterystyczne dla programistów ze wspaniałymi pomysłami, którzy nie chcą utrzymywać lokalnego centrum danych. Właściwie go nie mają i chcą jak najszybciej zabrać się do dzieła.
- **Myślenie startupowca**. Jest charakterystyczne dla kogoś, kto właśnie stracił pracę z powodu fuzji lub wykupu firmy i jest zdeterminowany do samodzielnego działania. Jego nowa firma nie dysponuje centrum danych, jednak ma w zanadrzu mnóstwo pomysłów, a zarazem brakuje mu gotówki.
- **Klient rządowy**. Dowiedzieliśmy się, że ze względu na oszczędności nasz resort rządowy przenosi się do chmury AWS w wyznaczonym czasie.

W każdym z powyższych przypadków panuje inne nastawienie do rozpoczęcia migracji lub projektowania infrastruktury chmury oraz hostowanych w niej aplikacji. Osoby pracujące w środowisku korporacyjnym lub rządowym prawdopodobnie oczekują od dostawcy usług w chmurze szczegółowej umowy o gwarantowanym poziomie świadczenia usług (SLA), którą można będzie dopasować do swoich potrzeb. Prawdopodobnie będą mieć także sprecyzowane oczekiwania dotyczące szczegółowości informacji o infrastrukturze i usługach dostawcy. W skrócie mówiąc, oczekują, że będą sprawować kontrolę nad tym procesem.

Jeśli ktoś rozpoczyna przygodę z dostawcą usług w chmurze jako programista indywidualny lub współpracujący ze startupem, prawdopodobnie nie może porównać przewidywanych kosztów z bieżącymi kosztami lokalnej infrastruktury. Zatem wszystkie koszty związane z usługami w chmurze zostaną na krótką metę zaakceptowane, lecz w miarę upływu czasu, wraz z nabywaniem doświadczenia, ogólne koszty chmury będą monitorowane i optymalizowane w celu maksymalnej redukcji.

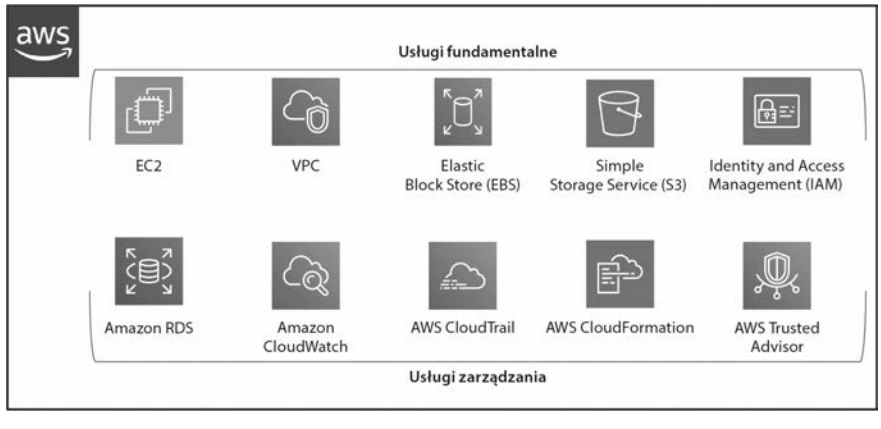
Uwaga

AWS udostępnia opcje dla programistów, którzy chcą dopasować i wdrożyć aplikacje hostowane w AWS. Na stronie *https://aws.amazon.com/startups/* można uzyskać dodatkowe informacje o zasadach kwalifikacji do programu o nazwie AWS Promotional Credit. W jego ramach można uzyskać kredyty w wysokości do 15 000 dolarów, do wykorzystania w ciągu 2 lat. Obejmują one także obsługę i szkolenia związane z usługami AWS.

W rzeczywistości przenosiny do chmury oznaczają oddanie pewnej części kontroli. W końcu to nie jest nasze centrum danych. W AWS nie zagłębiamy się w stos infrastruktury głębiej niż w podsieci, w których hostowane są nasze aplikacje. Pamiętajmy, że chmura jest centrum danych; nie jest to jedynie nasze centrum danych. Zacznijmy od zapoznania się z dostępnymi publicznie modelami obliczeniowymi w chmurze IaaS i PaaS, a także sprawdźmy, jak AWS się do nich dopasowuje.

Infrastruktura jako usługa

Większość usług dostępnych w AWS opiera się na modelu infrastruktury jako usługi (IaaS), zgodnie z rysunkiem 1.3. Jest to zdecydowanie najbardziej dojrzały model chmury spośród obecnie dostępnych; zwirtualizowane usługi i macierze dyskowe są hostowane w sieci zdefiniowanej programistycznie, przy czym infrastruktura każdego klienta jest całkowicie odizolowana jako zasób prywatny. Tworzenie zasobów w AWS zwykle zaczyna się od utworzenia tak zwanej wirtualnej chmury prywatnej (*Virtual Private Cloud* — VPC). W naszej izolowanej sieci prywatnej można hostować serwery wirtualne, woluminy na wirtualnych dyskach twardych oraz kompletne zarządzane usługi i produkty. W AWS możemy utworzyć dowolny stos architektoniczny za pomocą ogromnej liczby usług i narzędzi dostępnych w przyborniku IaaS. Firmy przenoszące się do chmury publicznej AWS zwykle zaczynają od IaaS, ponieważ usługi obliczeniowe i magazynowe odzwierciedlają ich bieżące lokalne środowisko wirtualne.



Rysunek 1.3. Infrastruktura jako usługa w AWS

Usługi w modelu IaaS w chmurze AWS są powiązane z usługami zarządzanymi. Zarządzana usługa opiera się na trójcy usług obliczeniowych, magazynowych i sieciowych, a także na specjalnie dostosowanym oprogramowaniu. W efekcie powstaje komponent, którego zarządzanie i utrzymanie chcemy powierzyć firmie Amazon, odciążając tym samym własną firmę. Przykładowo AWS oferuje zarządzaną usługę relacyjnej bazy danych (*Relational Database Service* — RDS). Za jej pomocą można zbudować, hostować, utrzymywać, tworzyć kopie zapasowe, konfigurować wznawianie pracy po awarii, synchronizować i monitorować główny i zapasowy serwer bazy danych. Użytkownik musi zadbać tylko o zarządzanie rekordami swoich danych. W AWS mamy do dyspozycji mnóstwo innych usług zarządzanych; w rzeczywistości wiele z nich nie wymaga ponoszenia dodatkowych kosztów. Przykładowo usługa automatyzacji o nazwie CloudFormation umożliwia automatyzację procedury tworzenia kompletnego stosu infrastruktury z potrzebnymi w aplikacji zasobami obliczeniowymi, magazynowymi i sieciowymi, a także modułem równoważenia obciążenia. W rzeczywistości CloudFormation umożliwia automatyzację praktycznie wszystkich zadań związanych z budowaniem, aktualizowaniem lub usuwaniem stosów infrastruktury w AWS. Bezpłatna jest też inna przydatna usługa o nazwie CloudTrail. Śledzi ona i rejestruje wywołania interfejsu programistycznego aplikacji (API), wykonywane przez wszystkie nasze konta w AWS w ciągu 90 dni. Oczywiście możemy skonfigurować CloudTrail, aby dane te zostały na zawsze zapisane w magazynie S3.

Aplikacje wewnętrzne działające w naszych lokalnych centrach danych są prawdopodobnie zróżnicowaną mozaiką własnościowych systemów operacyjnych (HP, AIX, Linux) oraz oczywiście systemu Windows. Wystarczy zasięgnąć języka w większości działów małych i średnich firm, aby zrozumieć, że większość pracowników nie darzy sympatią używanych aplikacji. Nauczyli się już rozwiązywać codzienne problemy związane z każdą z aplikacji. Porozmawiajmy z administratorami IT oraz z programistami korporacyjnych centrów danych; prawdopodobnie okaże się, że są bardzo niezadowoleni z braku elastyczności infrastruktury, którą muszą wykorzystywać i utrzymywać.

Prawdopodobnie, oprócz wspomnianych problemów, każdy dział firmy dysponuje własną infrastrukturą IT. Moja firma oferowała kiedyś usługi obliczeniowe dla średniej wielkości szpitala, wykorzystującego 25 odrębnych sieci. W większych korporacjach usługi obliczeniowe różnych działów są od siebie odseparowane, a każda linia biznesowa podejmuje własne decyzje.

W większości firm zatrudniających ponad 100 pracowników w serwerach wykorzystuje się jakiś rodzaj infrastruktury wirtualnej. Zwykle jest to VMware. Wirtualizacja miała rozwiązać problemy związane z kontrolowaniem kosztów infrastruktury ponoszonych przez firmy. Jednak hostowanie, uruchamianie i utrzymywanie usług wirtualizacji stało się niesłychanie drogie. Firmy zrozumiały, że koszty inwestycyjne oraz opłaty licencyjne należą do największych wydatków ponoszonych na stale rozrastającą się lokalną chmurę prywatną. Po zastąpieniu oprogramowania VMware serwerami i usługami wirtualnymi hostowanymi w AWS firmy nie potrzebują już specjalistów nadzorujących sprawy administracyjne. Ponadto aplikacje wykorzystywane przez korporacje są obecnie szeroko dostępne w chmurze publicznej jako aplikacje hostowane, dostępne w modelu oprogramowania

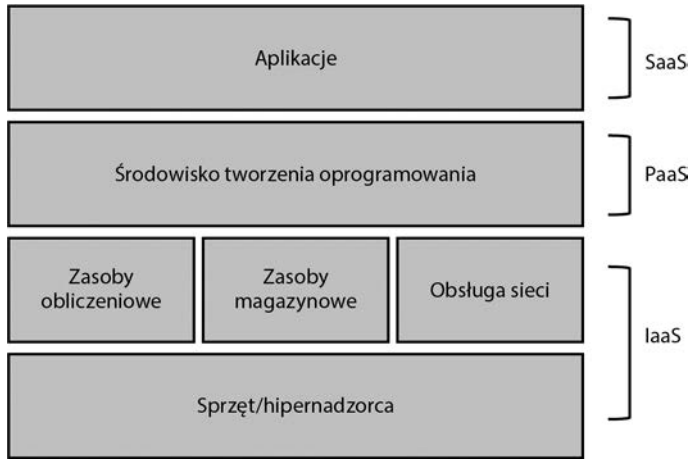
jako usługi (SaaS). W efekcie, na poziomie działów lub całej firmy rośnie zainteresowanie wykorzystaniem chmury publicznej do testowania aplikacji. W rzeczywistości może się okazać, że nie mamy wyboru. Jeśli korzystamy z produktów firmy Microsoft, najprawdopodobniej niektóre z codziennie używanych aplikacji, takich jak Exchange i Microsoft Office, są hostowane w Microsoft Azure i Office 365, dzięki czemu możemy nimi całkowicie zastąpić niektóre z aplikacji używanych w firmie. Więcej informacji o platformie obliczeniowej w AWS można znaleźć w rozdziale 4., „Usługi obliczeniowe — instancje EC2 w AWS".

Jeśli nasza firma nie ma żadnego doświadczenia w pracy z zewnętrznymi dostawcami usług w chmurze oraz można ją zaliczyć do kategorii średniej lub dużej korporacji, z pewnością pasuje do modelu prywatnej chmury. Większość infrastruktury firmy jest hostowana w kilku prywatnych centrach danych. Przykładowo główne centrum danych może się znajdować w Filadelfii, a inne w Nashville (w przypadku dość dużej firmy centra danych mogą się znajdować na kilku kontynentach). Wykorzystuje się w niej setki lub tysiące aplikacji. Możliwe, że firma ma szczęście i przestrzega się w niej scentralizowanych standardów IT, ale standardy te stały się problematyczne ze względu na aplikacje zainstalowane przez wiele oddziałów lub utworzone przez wiele lat. Być może firmie nie sprzyja szczęście, ponieważ jedna z najważniejszych aplikacji została napisana przez stażystę i włączona do produkcji bez większego zastanowienia.

W AWS zasoby infrastrukturalne są rozrzucone po całym świecie w 20 różnych regionach. Jeśli ktoś znajduje się w miejscu o wysokiej liczbie ludności, prawdopodobnie niedaleko umiejscowiona jest infrastruktura Amazona. Jeśli jednak nie, nadal można się do niej podłączyć za pośrednictwem jednej z lokalizacji brzegowych. Więcej informacji o regionach, strefach dostępności i lokalizacjach brzegowych można znaleźć w rozdziale 2., „Projektowanie z użyciem usług AWS Global Services".

Platforma jako usługa

Dostawcy rozwiązań chmurowych z kategorii platformy jako usługi (PaaS) umożliwiają programistom tworzenie własnych aplikacji z wykorzystaniem wielu popularnych platform programistycznych, takich jak Java, PHP i Python. Programiści nie muszą samodzielnie tworzyć komponentów infrastruktury wymaganych przez każdą aplikację; potrzebne zasoby infrastrukturalne są definiowane na początku cyklu programistycznego i zarządzane przez dostawcę rozwiązań chmurowych PaaS. Gdy napisane i przetestowane aplikacje są gotowe, udostępnia się je użytkownikom przy użyciu publicznych adresów URL. Dostawca rozwiązań PaaS będzie hostować i w miarę potrzeb skalować infrastrukturę. Środowiska PaaS są instalowane w zasobach IaaS dostawcy tych rozwiązań, zgodnie z rysunkiem 1.4. W rzeczywistości IaaS zawsze stoi u podstaw wszystkich rozwiązań typu „jako usługa". Przykładowymi dostawcami PaaS są Cloud Foundry i Heroku.



Rysunek 1.4. IaaS hostuje warstwę PaaS

Jeśli chodzi o Cloud Foundry, rozwiązanie PaaS stanowi podstawę rozwoju chmury IBM Cloud. W tym przypadku infrastruktura jest hostowana w publicznej chmurze IBM, na której uruchomiona jest odpowiednio dostosowana wersja komponentów platformy Cloud Foundry. Programiści mogą się zarejestrować i skoncentrować na pisaniu aplikacji. Wszystkie żądania zostaną obsłużone przez warstwę PaaS, stanowiącą interfejs warstwy IaaS, na której działają usługi obliczeniowe, magazynowe, równoważenia obciążenia i skalowania.

Innym popularnym rozwiązaniem stosowanym podczas tworzenia aplikacji w chmurze jest wspomniane wcześniej Heroku. Usługa ta umożliwia tworzenie i uruchamianie hostowanych aplikacji z wykorzystaniem wielu platform programistycznych. Podobnie jak w chmurze IBM, Heroku umożliwia hostowanie gotowej aplikacji, zapewnia równoważenie obciążenia i automatyczne skalowanie dostosowane do zapotrzebowania, a na koniec miesiąca wystawia rachunek za usługi.

Jeśli korzystamy z dostawcy PaaS, musimy pamiętać, że języki programowania od czasu do czasu się zmieniają; pociąga to za sobą zmiany w interfejsach API, które zwykle nie objawiają się ostrzeżeniami. Jeśli nasi programiści nie zadbają o aktualizacje, możemy się zetknąć z problemami wynikającymi z korzystania z platformy w chmurze PaaS.

Po zagłębieniu się w szczegółowe informacje w serwisie Heroku w sekcji Security przeczytamy, że „fizyczna infrastruktura Heroku jest hostowana i utrzymywana w bezpiecznych centrach danych firmy Amazon, a także wykorzystuje technologię Amazon Web Services". Heroku należy do Salesforce, innego dużego dostawcy usług w chmurze. Firma Salesforce poinformowała w roku 2018, że w ramach dalszego rozwoju będzie wykorzystywać zasoby centrów danych firmy Amazon. Ależ poplątana jest ta nasza sieć.

Warto sobie również uświadomić, że system PaaS jednego dostawcy nie musi być zgodny z usługą innego dostawcy rozwiązań w chmurze. Zarówno AWS, jak i Microsoft Azure oferują podobne usługi w chmurze, ale wewnętrznie każdy dostawca tych rozwiązań

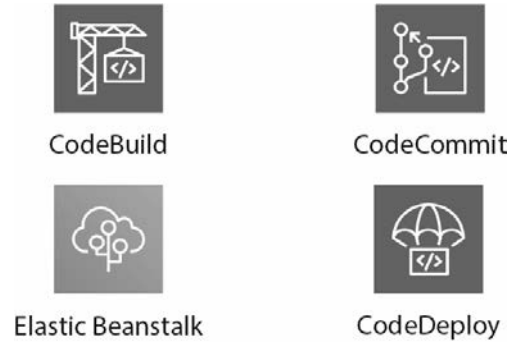
działa w zupełnie inny sposób, wykorzystując odmienny zestaw interfejsów API. Nie istnieje jeden standard definiujący cechy PaaS. Problemy ze zgodnością zaczynają się ujawniać na niższych poziomach rozwiązań proponowanych przez każdego dostawcę. Interfejsy typu REST, formaty plików manifestów, konfiguracje platform, zewnętrzne interfejsy API oraz integracja komponentów nie zawsze są zgodne z rozwiązaniami innych dostawców chmury. AWS radzi sobie z usługami platformowymi za pośrednictwem technologii Lambda, API Gateway oraz różnych narzędzi wdrażania kodu.

Aplikacje, które nasza firma być może tworzyła i wykorzystywała, charakteryzują się dwu- lub trójwarstwową architekturą z wieloma lokalnymi zależnościami, takimi jak magazyn sieciowy, magazyn lokalny, lokalni użytkownicy i bazy danych. Ogólny projekt architektury może się na początku sprawdzać, ale w pewnym momencie pojawią się problemy z działaniem ze względu na wiek i rozmiar sprzętu, a także na brak jakiejkolwiek elastyczności w odniesieniu do zmian.

Wyraźna różnica między oprogramowaniem lokalnym a hostowanym przez AWS polega na tym, że zamawianie i czekanie na sprzęt, a także na jego konfigurację odeszło do przeszłości. W rzeczywistości podczas projektowania aplikacji hostowanych w AWS można rozważyć wiele możliwości.

Wybór języka i platformy programistycznej wpłynie na wybór dostawcy PaaS. Dużo kodu napisano w Pythonie? Jesteś programistą Java? Amazon oferuje rozwiązanie PaaS o nazwie Elastic Beanstalk, które automatyzuje wdrażanie aplikacji utworzonych w językach Java, Python, Ruby i innych, w komponentach infrastrukturalnych wymaganych przez każdą aplikację, włącznie z instancjami EC2 lub kontenerami Dockera, modułami równoważenia obciążenia, automatycznym skalowaniem i monitorowaniem usług.

Amazon oferuje różne rozwiązania programistyczne, widoczne na rysunku 1.5, włącznie z CodeBuild, CodeCommit, Elastic Beanstalk, CodeDeploy. Mogą się one stać kluczowymi komponentami wdrażania aplikacji w AWS. W rozdziale 8., „Automatyzacja infrastruktury AWS”, opisałem działanie tych ciekawych zarządzanych usług, a także dodałem szczegółowe informacje o automatyzacji własnej infrastruktury.



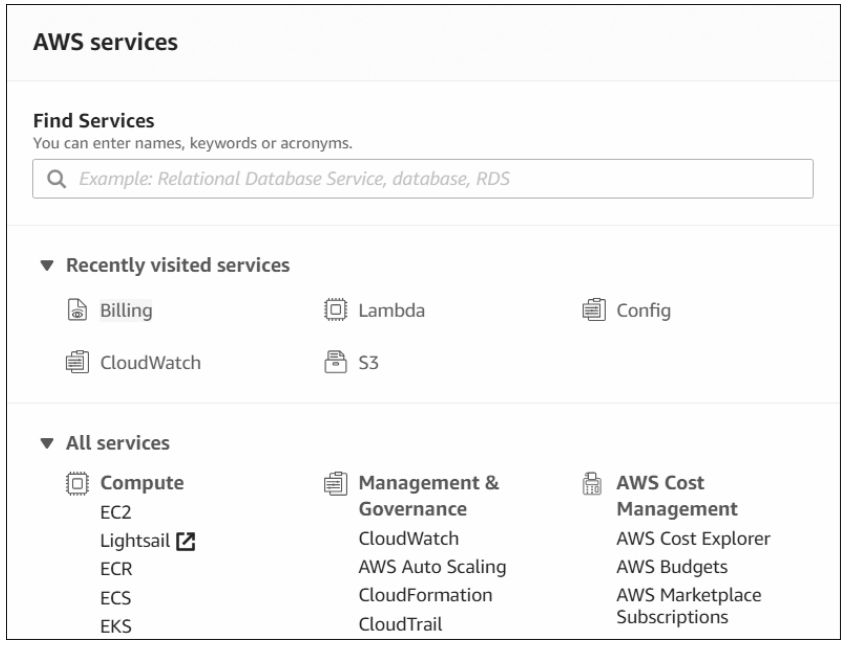
Rysunek 1.5. Opcje platform dostępnych w AWS

Główne cechy programowania w chmurze w AWS

Zapewne nie wszyscy słyszeli o amerykańskiej agencji rządowej NIST (*National Institute of Standards and Technology*). W 2010 roku instytut NIST rozpoczął prace nad dokumentacją chmury publicznej. Po przeprowadzeniu rozmów ze wszystkimi największymi dostawcami w czerwcu roku 2011 opublikował pierwszy raport, definiujący te komponenty, które okazały się wspólne dla wszystkich dostawców chmury publicznej. Raport można uznać za genialny, ponieważ zdefiniował cechy cieszącej się coraz większą popularnością chmury publicznej (kluczowe komponenty). W kolejnych latach definicje chmury opracowane przez NIST stały się standardem pracy z chmurą publiczną w wielu firmach. Pięć kluczowych definicji można uznać za standard w korzystaniu z chmury publicznej. Oto one.

Samoobsługa na żądanie. Od chmury publicznej nie tylko oczekujemy szybkiego dostarczenia, my go wymagamy. Wszyscy dostawcy chmury udostępniają samoobsługowy portal, tak samo jak AWS, zgodnie z rysunkiem 1.6. W portalu tym składamy wniosek o usługę w chmurze, a po kilku sekundach jest ona dostępna na naszym koncie AWS, gotowa do skonfigurowania. Bezpowrotnie minęły dni, gdy zamawialiśmy serwer wirtualny za pomocą poczty elektronicznej i czekaliśmy kilka dni na jego zbudowanie. W AWS serwer wirtualny można uruchomić i skonfigurować w ciągu kilku sekund. Zamówienie i uruchomienie zdefiniowanej programistycznie sieci w AWS (zwanej wirtualną chmurą prywatną) też jest kwestią kilku sekund. AWS oferuje rozszerzalną samoobsługową konsolę, za pomocą której możemy w kilka sekund zamówić i skonfigurować wiele usług w chmurze, w dowolnym regionie AWS. Wszystkie usługi w chmurze zamówione w AWS są automatycznie dostarczane za pośrednictwem silnie zautomatyzowanych procedur. Nie ma dostawców chmur publicznych, którzy nie udostępniają portalu wykorzystującego zautomatyzowane procesy działające w tle. Definicja opracowana przez NIST jest obecnie standardem.

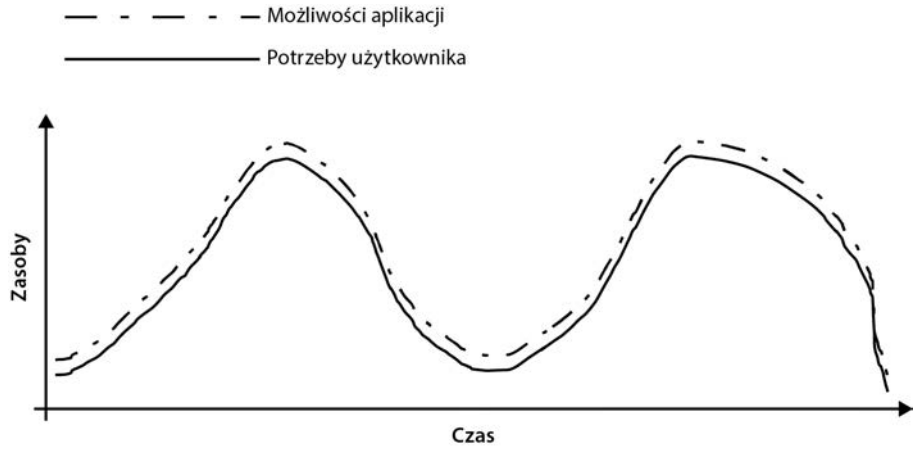
Szeroki dostęp sieciowy. Usługi w chmurze są dostępne niemal w każdym zakątku świata za pośrednictwem internetu. Jeśli hostujemy aplikacje w AWS, być może są to publiczne aplikacje SaaS. AWS oferuje także punkty końcowe HTTPS, umożliwiające dostęp do każdej usługi chmury hostowanej w AWS. Jednak nie wszyscy chcą korzystać z szerokiego dostępu sieciowego, czyli przy użyciu sieci publicznej, do swoich usług sieciowych. Okazuje się, że wiele firm przenoszących się do chmury AWS nie potrzebuje dostępu przez sieć publiczną do usług w chmurze. Chcą, aby ich usługi w chmurze pozostały prywatne i były dostępne tylko dla pracowników z wykorzystaniem połączenia prywatnego. Każdy klient chmury ostatecznie definiuje swoje znaczenie szerokiego dostępu sieciowego. W AWS aplikacje mogą być dostępne publicznie lub pozostać całkowicie prywatne. Często stosuje się połączenia VPN z miejsca pracy do AWS; w rzeczywistości można zamówić usługę Direct Connect i ustanowić prywatne połączenie światłowodowe z AWS, uzyskując połączenie o szybkości do 10 Gbps. Bez względu na typ aplikacji wykorzystywanych w chmurze szybki dostęp sieciowy jest podstawą. Możemy nawet używać usługi AWS, uzyskać do niej dostęp i zarządzać nią z poziomu telefonu, za pośrednictwem aplikacji AWS. Dostęp do AWS możemy uzyskać na każdym urządzeniu. Więcej informacji na temat sieci podaję w rozdziale 3., „Usługi sieciowe AWS”.



Rysunek 1.6. Portal zarządzania AWS

Pule zasobów. Zasoby infrastrukturalne dostawców chmury publicznej są zebrane w pule w wielu centrach danych, znajdujących się w różnych regionach świata, i są przydzielane automatycznie na żądanie. Firma wykorzystująca prywatną chmurę lokalną może utworzyć pulę maszyn wirtualnych, zasobów pamięci, procesów i usług sieciowych w jednym lub dwóch centrach danych, a następnie korzystać z własnej puli ograniczonych zasobów obliczeniowych. Wszyscy dostawcy chmury publicznej oferują ogromną pulę zasobów, które można wykorzystać na różne sposoby. AWS dysponuje klastrami centrów danych (zwanymi AZ lub strefami dostępności), a w każdej strefie AZ może funkcjonować ponad 80 000 fizycznych serwerów dostępnych online. Klienci mogą na nich hostować swoje usługi, zachowując gwarancję wysokiej odporności i wznawiania działania po awarii. Posiadanie wielu zasobów dostępnych online powoduje, że AWS może utrzymywać niskie ceny. Bez ogromnej puli zasobów nie udałoby się zaoferować w AWS usług w chmurze na żądanie, z możliwością ich skalowania w zależności od potrzeb klienta. Posiadanie ogromnej puli zasobów jest niezbędnym standardem dla wszystkich publicznych dostawców chmury; klienci nie są przygotowani na brak dostępności zasobów. Przykładem może być magazyn AWS S3 będący usługą, w której nie zdefiniowano maksymalnego limitu danych. Więcej informacji o regionach i strefach AZ znajduje się w rozdziale 2.

Szybka elastyczność. Elastyczność, inaczej skalowalność, chmury publicznej jest *kluczową* cechą wymaganą przez wszystkie aplikacje hostowane w chmurze. Elastyczność w AWS jest cechą zarówno funkcji obliczeniowych, jak i magazynowych. Ponieważ większość usług i aplikacji wymaga przeprowadzania obliczeń oraz magazynowania, aplikacje w chmurze AWS mogą się automatycznie skalować, zgodnie z rysunkiem 1.7.

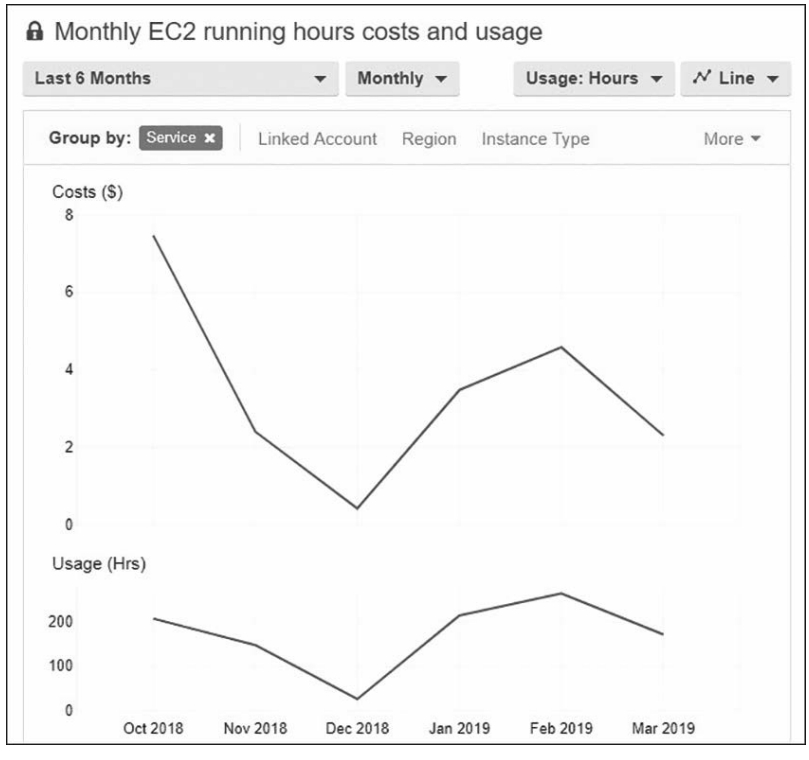


Rysunek 1.7. Aplikacje w chmurze publicznej mogą się skalować na żądanie

Warto podkreślić, że elastyczność czy też skalowalność przydaje się tylko wtedy, kiedy jest zautomatyzowana pod kątem wymagań. Nie interesuje nas elastyczność polegająca na wyłączeniu serwera wirtualnego, dodaniu do niego pamięci RAM i ponownym włączeniu; potrzebna jest skalowalność pozioma, czyli więcej serwerów aplikacji, a nie po prostu większy serwer. Monitorowanie w czasie rzeczywistym aplikacji hostowanej w chmurze AWS umożliwia niemal natychmiastową reakcję, zanim jeszcze wydajność aplikacji zbliży się do granic możliwości. Dzięki usłudze automatycznego skalowania EC2 (EC2 Auto Scaling), uruchomionej w tle, automatycznie zamawiane są dodatkowe zasoby komputerowe, przydzielane następnie do klastra serwera aplikacji, zatem aplikacja nie traci wydajności. Szybką elastyczność na żądanie można osiągnąć jedynie za sprawą monitorowania w czasie rzeczywistym, które umożliwia automatyczne skalowanie. To przyczynia się do tak wielkiej popularności chmury publicznej: ogromna pula dostępnych zasobów w chmurze oraz możliwości automatycznego skalowania aplikacji na żądanie powodują, że w AWS każdy może z łatwością skalować stos aplikacji w górę lub w dół. Więcej informacji o wdrażaniu skalowalności i elastyczności za pomocą funkcji EC2 Auto Scale, znajduje się w rozdziale 5., „Planowanie w celu zapewnienia skalowania i odporności".

Usługa opomiarowana. W chmurze dostajemy rachunek tylko za faktyczne wykorzystanie zasobów; jest to tak zwana usługa opomiarowana. Dostawcy usług w chmurze zarabiają, pobierając opłaty za wszystko, z czego korzystamy w ich centrach danych, włącznie z kosztem transferu danych. Przesyłanie danych do chmury publicznej jest zwykle bezpłatne; przesyłanie danych poza chmurę, a także między podsieciami hostowanymi w różnych centrach danych, jest zwykle obciążone opłatą za dane wysyłane poza chmurę. W przypadku usług obliczeniowych, takich jak instancje obliczeniowe AWS EC2, opłaty są naliczane za każdą sekundę lub minutę. Natomiast w usługach magazynowych, takich jak S3 lub wirtualne dyski twarde, które w AWS są nazywane elastycznym magazynem blokowym (*Elastic Block Storage* — EBS), płacimy za liczbę gigabajtów wykorzystanych

w każdym miesiącu. AWS może naliczać opłaty za funkcje obliczeniowe, magazynowanie i przesyłanie danych. Licznik opłat działa, kiedy usługa AWS jest włączona. Zarządzanie kosztami jest jednym z najważniejszych zadań związanych z wykorzystaniem chmury. AWS oferuje wiele przydatnych narzędzi ułatwiających kontrolowanie kosztów. Są to między innymi AWS Simple Monthly Calculator, AWS Budgets i Cost Explorer, widoczne na rysunku 1.8 i opisane szczegółowo w rozdziale 2. Opłaty za usługi w chmurze są faktem, do którego wszyscy przywykliśmy. Będziemy też musieli przywyknąć do czynników wpływających na wysokość rachunku. Właśnie dlatego powinniśmy zrozumieć i z uwagą monitorować koszty obliczeń, magazynu oraz transferu danych. Przykładowo w AWS możemy zamówić usługę równoważenia obciążenia za 30 dol. miesięcznie. Warto jednak zauważyć, że dodatkowo musimy zapłacić za transfer wszystkich danych przez moduł równoważenia obciążenia, co może się okazać bardzo kosztowne.



Rysunek 1.8. Usługi AWS Budgets i Cost Explorer śledzą koszty i powiadamiają o przekroczeniu budżetu

Operacyjne korzyści wynikające z używania AWS

Działalność w chmurze publicznej przynosi różnorakie korzyści. Nieograniczony dostęp do serwerów, magazynu oraz do wielu usług zarządzania sprawia, że prowadzenie działalności w chmurze jest łatwiejsze niż wiele osób myśli. W tabeli 1.1 podsumowałem usługi zarządzane dostępne w AWS, które mogą zastąpić lub uzupełnić lokalne usługi i procedury.

Serwery. Niedostatecznie wykorzystane serwery w naszym centrum danych są drogie w działaniu i utrzymaniu. Przeniesienie aplikacji do chmury publicznej zmniejszy lokalne centrum danych. Ponieważ nie będziemy już utrzymywać tylu serwerów fizycznych, całkowity koszt hostingu (ogrzewania, chłodzenia itd.) również spadnie. To samo dotyczy opłat za licencje na oprogramowanie, ponieważ nie będziemy już odpowiadać za usługi hipernadzorcy, gdyż jest to zadanie firmy Amazon. Ktoś może sobie pomyśleć, że przeniesienie do chmury AWS wiąże się z koniecznością wirtualizacji zasobów. Jednak AWS oferuje wiele opcji obliczeniowych, z wirtualizacją dowolnego rozmiaru i skali, od jednordzeniowego procesora z 512MB pamięci RAM, po procesory z setkami rdzeni i terabajtami pamięci RAM. Można też zamówić i dowolnie wykorzystywać serwery fizyczne. Więcej informacji o opcjach obliczeniowych znajduje się w rozdziale 4.

Magazyn. Korzystanie z magazynu w chmurze przynosi wiele korzyści ze względu na jego nielimitowany rozmiar, gwarantowany przez dostawców chmury. Amazon oferuje wiele opcji magazynowania, podobnych, lecz nieidentycznych z rozwiązaniami lokalnymi. W przypadku magazynu sieciowego Amazon oferuje systemy plików współdzielonych: elastyczny system plików (*Elastic File System* — EFS) dla systemu Linux oraz FSx, czyli usługę plików współdzielonych dla serwera plików Windows. Za pośrednictwem EBS dostępne są wirtualne dyski twarde. Usługi S3 i S3 Glacier zapewniają nieograniczony magazyn oraz długotrwały magazyn archiwum. Więcej informacji o opcjach przechowywania danych w AWS podano w rozdziale 6., „Magazyn w chmurze".

Usługi zarządzane. AWS oferuje wiele usług zarządzanych, zgodnie z tabelą 1.1. Po przeniesieniu się do chmury mogą one zastąpić lub uzupełnić wykorzystywane w firmie usługi i narzędzia.

Ograniczenia dostawców chmury

Każdy dostawca chmury publikuje treść SLA, czyli umowy o gwarantowanym poziomie świadczenia usług, w której określa dostępność usług na różnych poziomach operacyjnych. Wszyscy dostawcy chmury publicznej składają obietnice dotyczące bezpieczeństwa, zgodności i ogólnego działania, a także opisują, jak ich metodologia wpisuje się w te zasady. Wyzwanie polega na dotrzymaniu tej umowy. W SLA znajdziemy szczegóły dotyczące akceptowalnego czasu przerwy w działaniu usługi oraz opis odpowiedzialności dostawcy chmury na wypadek wystąpienia tej przerwy. Umowa będzie także zawierać ustalenia dotyczące braku odpowiedzialności za zdarzenia będące poza kontrolą dostawcy. Innym typowym terminem używanym w SLA jest „dołożenie wszelkich starań" lub „uzasadnione ekonomicznie starania".

Tabela 1.1. *Usługi zarządzane w AWS*

Operacje IT	Lokalne	Chmura AWS
Monitorowanie	Nagios, SolarWinds	Monitoring za pośrednictwem usługi CloudWatch, zapewniającej metryki dla wszystkich usług AWS. Wszystkie dane z monitoringu i dzienników można przechowywać w magazynie S3. Wszystkie zewnętrzne rozwiązania monitorowania mogą uzyskać dostęp do S3 i przeprowadzić własne analizy zebranych danych.
Tworzenie kopii zapasowych danych	Narzędzia do tworzenia kopii zapasowych, takie jak Commvault i NetBackup	Każdy dostawca zewnętrzny, który chce pozostać na rynku, zapewnia obsługę AWS; zarówno Veritas, jak i Commvault oferują rozwiązania AWS. Można też zainstalować AWS Storage Gateway, aby lokalnie zapisywać potrzebne dane, a zarazem tworzyć kopie zapasowe lokalnych dysków na S3. Kopie zapasowe mogą być migawką lokalnych wirtualnych dysków twardych lub plików danych z konkretnych woluminów.
Skalowanie	Dodawanie kolejnych maszyn wirtualnych lub zwiększenie czy zmniejszenie rozmiaru pamięci i liczby rdzeni każdej maszyny wirtualnej	Skalowanie poziome przy użyciu wielu maszyn wirtualnych (instancji) na potrzeby równoważenia obciążenia, a także dodanie skalowania automatycznego, w zależności od wymagań w celu zwiększenia lub zmniejszenia wymaganych mocy obliczeniowych z wykorzystaniem funkcji EC2 Auto Scaling.
Testowanie	Zapewnienie sprzętu niezbędnego do testowania jest kosztowne	Zapewnienie zasobów do testów krótkoterminowych w AWS jest niesłychanie tanie. Po zarejestrowaniu się w darmowym planie AWS można przez jeden rok za darmo testować różnorodne usługi AWS.
Zarządzanie tożsamością	Usługi Active Directory Domain Services służące do uzyskania dostępu do zasobów korporacji	Można rozszerzyć lokalne instancje Active Directory na chmurę AWS, hostującą usługi katalogowe. Za pośrednictwem usług pojedynczego logowania (*Single Sign-On* — SSO) AWS można zarządzać dostępem do popularnych aplikacji biznesowych, hostowanych przez zewnętrznych dostawców chmury.

Dostawca chmury, niezależnie od jej modelu, odpowiada za ogólne działanie i wdrożenie usługi, orkiestrację, ogólne zarządzanie chmurą, bezpieczeństwo komponentów chmury i zapewnienie prywatności klienta. Umowa SLA w pewnym stopniu określa także odpowiedzialność za relacje biznesowe między każdym klientem a dostawcą chmury. Każdy klient musi w pełni rozumieć ofertę związaną z poszczególnymi usługami w chmurze; musi wiedzieć, czego oczekiwać po każdej usłudze.

W rzeczywistości nie każdy dostawca chmury publicznej oferuje zadowalającą umowę SLA. Okazuje się, że „dołożenie wszelkich starań" oznacza zwykle, że firmy te po prostu zaoferują to, co mają najlepsze. Być może nie brzmi to zbyt łagodnie, ale taka jest prawda; zgodnie z AWS „wszystko się cały czas psuje". Co się stanie, gdy kluczowy komponent

aplikacji hostowanej w chmurze AWS zawiedzie? Czy będzie to katastrofa, czy sobie z tym poradzimy? Czy zaakceptujemy występujące czasem awarie AWS? Taka jest rzeczywistość; AWS ma całkowitą rację: wszystko się psuje.

Korzystanie z chmury publicznej oznacza, że musimy tak zaprojektować hostowaną aplikację, aby działała nawet podczas wystąpienia awarii usług obliczeniowych i magazynu. Jest to nasza odpowiedzialność.

Wszyscy dostawcy chmury publicznej oferują SLA o takiej samej treści; oto ona, skrócona do kilku krótkich słów: „Przykro nam; jako rekompensatę oferujemy zniżkę na nasze usługi". To podsumowanie treści SLA dotyczy każdego dostawcy chmury publicznej. Oto inny przykład: jeśli przytrafi się nam awaria, będziemy musieli ją udowodnić, przedkładając rejestry ruchu sieciowego oraz odpowiednią dokumentację, która nie pozostawi żadnych wątpliwości, że problemy naszej aplikacji są skutkiem problemów z chmurą AWS.

Musimy jeszcze pamiętać o jednym drobnym szczególe: jeśli w projekcie aplikacji nie uwzględni się nadmiarowości, nie warto się nawet starać o zniżkę. Projekt aplikacji, która jest hostowana na jednej instancji, bez zapewnienia wznawiania działania po awarii ani bez gwarancji wysokiej dostępności, nie jest objęty umową SLA. AWS oczekuje, że poważnie podchodzimy do projektu swojej aplikacji. Musimy rozumieć i wykorzystywać odpowiednie narzędzia z przybornika AWS, aby spełnić warunki SLA dotyczące dostępności i wydajności.

Warunki SLA nie są zdefiniowane dla wszystkich usług AWS; istnieje ponad 100 usług i jedynie 8 zdefiniowanych umów SLA. Trzeba pamiętać, że wszystkie usługi zarządzane, czyli właściwie wszystkie, jakie mamy do dyspozycji, opierają się na zasobach opisanych w tabeli 1.2.

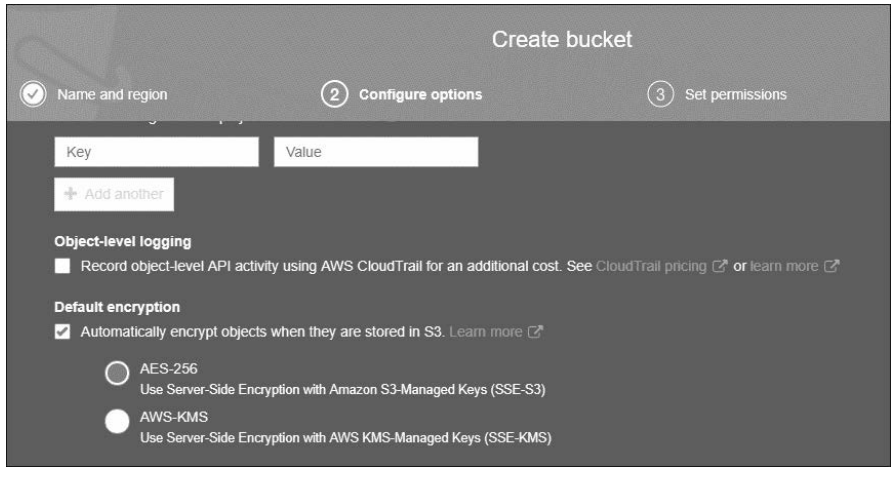
Tabela 1.2. *Warunki SLA w AWS*

Usługa AWS	Podsumowanie SLA
CloudFront	99,9% podczas każdego miesięcznego cyklu płatniczego
DynamoDB	Miesięczny czas działania na poziomie 99,999% w przypadku tabel globalnych lub 99,99% w przypadku zwykłych tabel
Instancje EC2 (włącznie z usługą ECS i woluminami EBS)	Miesięczny czas działania na poziomie co najmniej 99,99%
Bazy danych RDS	Miesięczny czas działania na poziomie co najmniej 99,95% w przypadku instancji zlokalizowanych w wielu AZ
Usługa DNS Route 53	Uzasadnione ekonomicznie działania mające na celu zapewnienie 100% dostępności usługi Route 53 podczas miesięcznego okresu płatniczego
S3; magazyn obiektów S3 Glacier	Miesięczny czas działania na poziomie co najmniej 99,9%
Funkcje Lambda	Miesięczny czas działania na poziomie 99,95% podczas miesięcznego okresu płatniczego
AWS Shield (Advanced)	Każdy przypadek niedopełnienia warunków usług CloudFront lub Route 53 podczas ochrony przez AWS Shield Advanced przeciwko atakom typu DDoS (*Distributed Denial of Service*) stanowi naruszenie postanowień umowy SLA.

Bezpieczeństwo danych w AWS

Podczas działania w chmurze możemy wiele stracić: instancje ulegają awarii, woluminy EBS się zawieszają, usługi przestają działać. Nie możemy jednak iść do szefa i oznajmić, że utraciliśmy jakieś dane.

Bezpieczeństwo danych. W rzeczywistości nasze dane będą bezpieczniejsze i trwalsze, jeśli umieścimy je w chmurze publicznej. Wszystkie media magazynowe w AWS domyślnie nie są szyfrowane, z wyjątkiem magazynu archiwum S3 Glacier, który jest automatycznie szyfrowany. Jednak woluminy EBS — zarówno rozruchowe, jak i woluminy danych — można zaszyfrować podczas przechowywania i transferu. W tym celu wykorzystuje się klucze główne dostarczane przez AWS lub klucze dostarczane przez klienta. Usługi współdzielonego magazynu, na przykład EFS, mogą też zapewnić szyfrowanie w stanie spoczynku. To samo dotyczy tabel DynamoDB. Kontenery S3 można zaszyfrować za pomocą kluczy zapewnianych przez AWS lub klientów, zgodnie z rysunkiem 1.9. Trwałość danych jest zabezpieczeniem innego typu; wszystkie dane zgromadzone w chmurze są przechowywane w wielu lokalizacjach; woluminy EBS są replikowane w centrum danych, w którym się znajdują. Obiekty S3 są replikowane w trzech oddzielnych lokalizacjach w wybranym regionie AWS, co zapewnia wysoki poziom trwałości. Poziom trwałości S3 oferowany przez Amazon żartobliwie określa się następująco: co 10 milionów lat tracimy jeden obiekt na 1000 obiektów przechowywanych w S3. Prawdopodobnie nie zdołamy uzyskać tego poziomu trwałości i bezpieczeństwa w lokalnej infrastrukturze.



Rysunek 1.9. Kontenery S3 można zaszyfrować za pomocą kluczy zarządzanych AES-256 lub AWS-KMS

Prywatność danych. W AWS nie istnieje osobny magazyn danych dla poszczególnych klientów; wszystkie serwery magazynu w AWS są zaprojektowane z myślą o wielu klientach. Jest to właściwie domyślna konfiguracja u wszystkich dostawców chmury publicznej. Zadaniem Amazona jest zapewnienie izolacji rekordów danych w obrębie konta AWS.

Kontrola danych. Klienci mają pełną kontrolę nad przechowywaniem i pobieraniem swoich danych zgromadzonych AWS. Wszystkie magazyny danych w AWS są domyślnie prywatne i z wyjątkiem kontenerów S3, które można skonfigurować jako publiczne, pozostają prywatne i nie są bezpośrednio dostępne z zewnątrz. Klienci mogą udostępnić publicznie kontenery S3; to do nich należy odpowiedzialność za bezpieczeństwo i dostępność wszystkich rekordów danych przechowywanych w AWS.

Kontrola nad bezpieczeństwem. Jak wcześniej wspominałem, w AWS można zaszyfrować wszystkie rekordy danych. Zasady definiujące precyzyjny poziom bezpieczeństwa i dostępu do zasobów można bezpośrednio powiązać z kontenerami S3 lub ze współdzielonym magazynem EFS. Zasady te można definiować, korzystając z zasad bezpieczeństwa usługi zarządzania tożsamością i dostępem (*Identity and Access Management* — IAM).

Zasady tożsamości i zaufania IAM można zdefiniować na różnych poziomach szczegółowości. W ten sposób możemy kontrolować dostęp użytkowników i ról do *wszystkich* zasobów w AWS, włącznie z *dowolnym* magazynem. Szczegółowe informacje o IAM zawiera rozdział 7., „Usługi bezpieczeństwa".

Aby zapewnić kontrolę nad usuwaniem rekordów danych, kontenery S3 można dodatkowo zabezpieczyć, włączając uwierzytelnianie wieloskładnikowe.

Bezpieczeństwo sieciowe w AWS

Konfiguracja sieci w AWS odbywa się na poziomie podsieci. Wszystkie podsieci tworzy się jako prywatne, bez dostępu do świata zewnętrznego. Podsieci znajdują się w naszych sieciach prywatnych, które w AWS noszą miano wirtualnych chmur prywatnych (*Virtual Private Cloud* — VPC). Podsieci można udostępnić za pośrednictwem internetu lub prywatnego połączenia VPN z sieci lokalnej. W tym celu należy dodać do VPC usługę bramy. Zagadnienia sieciowe w AWS są opisane w rozdziale 3.

Należy koniecznie zauważyć, że wybór publicznych i prywatnych połączeń należy do każdego klienta; nie leży to w gestii AWS.

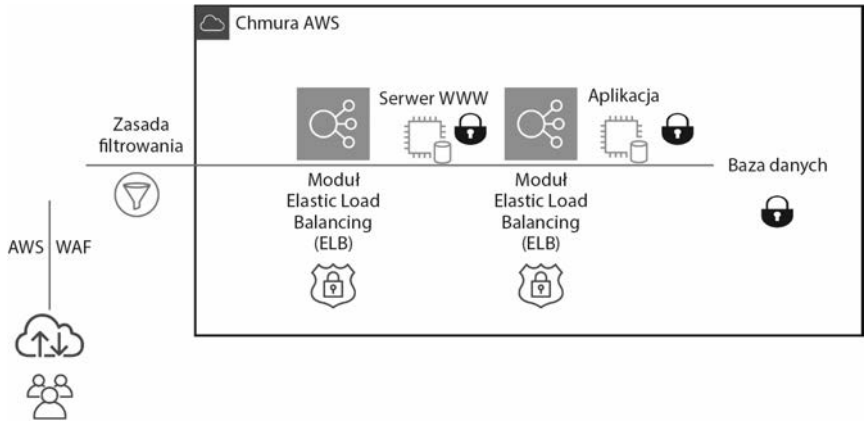
- Ruch przychodzący i wychodzący w każdej podsieci można kontrolować za pośrednictwem zapory sieciowej o nazwie Network ACLs, która definiuje osobne reguły bezstanowe dla przepływu pakietów przychodzących i wychodzących.
- Każda instancja EC2 hostowana w podsieci jest chroniona przez dodatkową zaporę sieciową zwaną grupą bezpieczeństwa, która definiuje, jaki ruch może się przedostać do instancji i gdzie należy przekierować ruch wychodzący.

Jeśli włączymy dzienniki przepływu VPC, możemy rejestrować ruch dla całej chmury VPC, jednej podsieci lub interfejsu sieciowego.

Bezpieczeństwo aplikacji w AWS

Hostowane w AWS serwery sieciowe i serwery aplikacji zawsze powinny znajdować się w podsieciach prywatnych. Podsieci prywatne nie są bezpośrednio dostępne w internecie. Możemy się zastanawiać, jak uzyskać dostęp do aplikacji, która miała być w zamierzeniu dostępna publicznie, a która nie ma bezpośredniego dostępu publicznego. Rozwiązaniem jest zdecydowanie najlepsza praktyka, jakiej należy przestrzegać w AWS. Jeśli jakiś serwer WWW powinien być dostępny dla klientów przez internet, wówczas w sieci publicznej należy umieścić moduł równoważenia obciążenia, przekierowujący ruch do serwera WWW. Jest to poprawne rozwiązanie projektowe. Klienci, którzy chcą uzyskać dostęp do aplikacji, zostaną przekierowani przez usługę DNS do nazwy DNS modułu równoważenia obciążenia. Moduł ten przekieruje ruch przychodzący z podsieci publicznej do docelowych serwerów WWW, hostowanych w podsieciach prywatnych.

Jednym z modułów równoważenia obciążenia dostępnych w AWS jest Application Load Balancer. Usługa ta może zapewnić uwierzytelnianie i usługi redukcji obciążenia SSL. Wzorzec ruchu typu end-to-end dla trójwarstwowej aplikacji można zaprojektować z wykorzystaniem wielu punktów szyfrowania i rozszyfrowywania, znajdujących się na trasie ruchu z miejsca źródłowego do docelowego. Zostało to przedstawione na rysunku 1.10.



Rysunek 1.10. Przepływ zaszyfrowanych danych w AWS

- **Zapora sieciowa aplikacji WWW**. Jest to niestandardowy filtr ruchu, umieszczony przed usługą Application Load Balancer, chroniący przed ruchem o złośliwym pochodzeniu.
- **Elastic Load Balancer (ELB)**. Akceptuje tylko zaszyfrowany ruch HTTPS na porcie 443; zapewnia szyfrowanie protokołów *Secure Sockets Layer/Transport Layer Security* (SSL/TLS) oraz opcjonalnie uwierzytelnianie użytkownika.
- **Instancja EC2 hostująca aplikację WWW**. Można zaszyfrować dyski rozruchowe EBS oraz dyski danych.

- **Instancja EC2 hostująca serwer aplikacji**. Można zaszyfrować dyski rozruchowe EBS oraz dyski danych.
- **Serwer bazy danych**. Dyski rozruchowe EBS, dyski danych oraz dane społeczności można zaszyfrować. Można też zaszyfrować tabele Dynamo DB.

Zgodność w chmurze AWS

Jako światowy dostawca chmury publicznej AWS działa w różnych krajach i podlega wielu zasadom oraz regulacjom nakładanym przez rządy, a także wynikającym ze standardów zgodności. W zależności od typu naszej działalności, korzystając z chmury AWS, będziemy musieli dostosować się do różnych poziomów zgodności. Instytucje finansowe, służba zdrowia i instytucje rządowe przestrzegają ścisłych reguł, do których muszą się stosować ich klienci. Ponadto nasza firma może przestrzegać określonych reguł wewnętrznych.

Wiele krajów na świecie ustanawia prawa, regulacje i nakazy, przywiązując dużą wagę do ochrony prywatności danych osobistych, a także do bezpieczeństwa informacji korporacyjnych i systemów komputerowych. Nowe prawo ochrony danych nakłada konieczność zapewnienia ochrony i bezpieczeństwa danych na ich nadzorcę, czyli na miejsce przechowywania danych podczas transferu z miejsca źródłowego do docelowego.

Dostawcy usług w chmurze są zobowiązani do przestrzegania zapisów z SLA w odniesieniu do danych przechowywanych w chmurze przez organizacje. Niektóre z typowych regulacji zgodności, które zostały pomyślnie zweryfikowane w AWS, dotyczą standardów opisanych w tabeli 1.3.

Tabela 1.3. *AWS obsługuje wiele standardów zgodności*

Skrót	Zakres działania	Cel ochrony	Stan prawny
HIPAA	Służba zdrowia	Dane osobowe	Ustawa
GLBA	Branża finansowa	Dane osobowe	Ustawa
SOX	Spółki publiczne	Udziałowiec	Ustawa
PCI DSS	Branża kart płatniczych	Oszustwo	Regulacja branżowa
RODO	UE	Dane osobowe	Ustawa

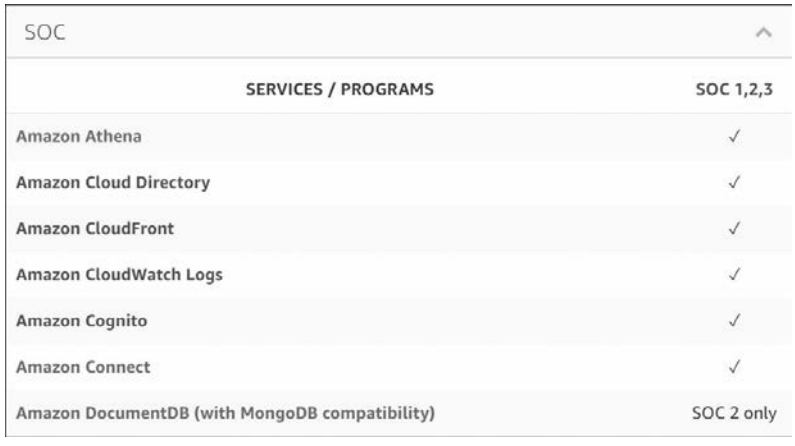
Health Insurance Portability and Accountability Act — zabezpiecza prywatność rekordów dotyczących informacji zdrowotnych w Stanach Zjednoczonych.

Gramm-Leachy-Billy Act — nakazuje ochronę informacji klientów przez branże finansowe.

Sarbanes-Oxley — zapewnia integralność operacji finansowych w spółkach publicznych.

PCI DSS — zapewnia integralność przetwarzania danych kart kredytowych lub danych uwierzytelniających.

RODO — chroni prywatność i dane osobowe wszystkich obywateli UE. Amazon opracował porządną stronę dotyczącą prywatności (*https://aws.amazon.com/compliance/*), na której znajdują się szczegółowe informacje o certyfikacji oraz atestach, jakie uzyskał lub jakie obsługuje AWS. Jeśli musimy przestrzegać określonych standardów zgodności, jednym z pierwszych kroków powinno być przejrzenie usług AWS dostępnych dla każdego standardu zgodności, co widać na rysunku 1.11.



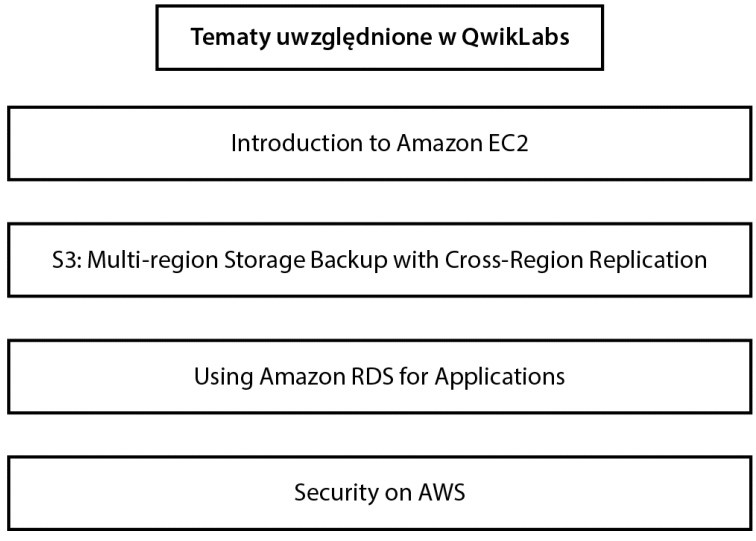
Rysunek 1.11. Na stronie poświęconej zgodności w AWS można sprawdzić obsługę określonych usług

Korzystanie z piaskownicy AWS

AWS ułatwia „wypróbowanie przed zakupem", często kierując oferty promocyjne do programistów. Jeśli nawet ktoś nie jest programistą, to jako nowy klient AWS uzyska na jeden rok darmowy dostęp do niemal wszystkich usług AWS (Amazon nazywa ten dostęp „free tier"). Jest to świetny sposób na wypróbowanie AWS. Należy jedynie podać dane karty kredytowej, która jednak nie zostanie obciążona, o ile nie zdecydujemy się skorzystać z zasobów spoza bezpłatnej oferty. Po upływie pierwszego roku zostaniemy obciążeni kosztami wszystkich wykorzystywanych usług; wszystkie zasoby utworzone w AWS w trakcie pierwszego roku pozostaną do naszej dyspozycji, ale zaczną być za nie naliczane opłaty.

Ponadto w AWS dostępnych jest kilka bezpłatnych laboratoriów praktycznych. Pod adresem *https://run.qwiklabs.com/* można się zarejestrować w serwisie QwikLabs i wykonać różne zadania w chmurze AWS.

Rysunek 1.12 przedstawia kilka opcji nauki i laboratoriów dostępnych w serwisie QwikLabs.



Rysunek 1.12. W QwikLabs mamy do dyspozycji ponad 20 zupełnie darmowych laboratoriów związanych z usługami AWS

Podczas wykonywania eksperymentów i ćwiczeń dostępnych w laboratoriach nasuną się pytania, które ułatwią poszerzanie wiedzy i doświadczenia związanego z chmurą AWS.

Obejrzyj film dołączony do książki „SIGNING UP FOR AWD FREE TIER".

Jaki problem chcemy rozwiązać?

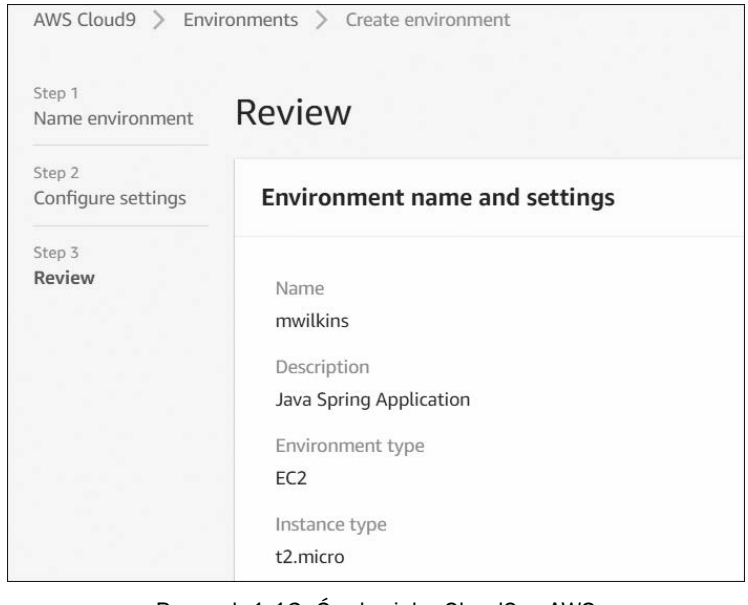
Zwykle w wielkich organizacjach wykorzystuje się setki lub tysiące aplikacji działających na serwerach wirtualnych. Które aplikacje można przenieść do AWS? Jakie są priorytety?

Przenosiny do chmury AWS zacznijmy od aplikacji o niskiej wartości lub niskim poziomie ryzyka. Zwykle zaleca się na początek wybór najbardziej wartościowej aplikacji, która zarazem jest obarczona najniższym ryzykiem. Jednak rzeczywistość weryfikuje te zalecenia: prawdopodobnie przeniesienie aplikacji do chmury zajmie co najmniej 6 miesięcy. Wybór aplikacji o niskiej wartości zapewni cenny czas, który będziemy mogli poświęcić na dodatkowe planowanie i analizy, zanim ostatecznie skonfigurujemy aplikację w AWS. Spotkałem się z wieloma firmami, które twierdziły, że szybko przeniosą swoje aplikacje do chmury. Rzadko kończy się to powodzeniem, ponieważ należy się wielu rzeczy nauczyć i przeprowadzić sporo analiz. Zacznijmy od aplikacji o niskiej wartości. Poświęćmy na to tyle czasu, ile trzeba, i wybierzmy aplikację, która z powodzeniem działała przez długi czas. Następnie można udokumentować zdobyte doświadczenie i określić, co należy zmienić następnym razem. Wtedy przeniesienie drugiej i trzeciej aplikacji do chmury odbędzie się znacznie szybciej.

Utwórzmy zupełnie nową aplikację. Zaletą utworzenia zupełnie nowej aplikacji w AWS jest brak jakichkolwiek ograniczeń, takich jak konieczność użycia określonego rodzaju bazy danych, języka programowania lub sposobu przeprowadzania obliczeń. Jeśli korzystanie z AWS rozpoczniemy od zupełnie nowej aplikacji, będziemy mogli wypróbować nowe metody hostowania aplikacji, na przykład obliczenia bezobsługowe, tworzenie aplikacji mobilnej z wykorzystaniem komponentów bezstanowych lub użycie DynamoDB zamiast SQL. W ten sposób szybko dowiemy się, co ma do zaoferowania chmura AWS.

Spróbujmy rozwiązać jeden problem. Czy potrzebujemy dodatkowego magazynu? Prawdopodobnie jest to świetny moment na rozpoczęcie przygody z chmurą. Aby zarchiwizować pliki w S3 Glacier, wystarczy zamówić urządzenie Snowball, połączyć je z siecią, skopiować pliki do archiwizacji i wysłać do AWS. Jest to doskonały pierwszy projekt, w którym możemy zacząć korzystać z obsługi AWS, archiwizować rekordy i oszczędzać pieniądze firmy.

Zdefiniujmy wartościowy cel. W idealnym scenariuszu przeniesienie do AWS jest długoterminowe i zakończone powodzeniem. Tysiące firm z powodzeniem przeniosły się do AWS; również my możemy się o tym przekonać. Zacznijmy od zdefiniowania jakiegoś celu, który można szybko zweryfikować, raczej w ciągu kilku miesięcy niż lat. Jeśli przykładowo chcemy utworzyć aplikację, możemy się zarejestrować w usłudze Cloud9 AWS, czyli w środowisku IDE hostowanym w chmurze, obsługującym ponad 40 języków programowania, przedstawionym na rysunku 1.13. Wyposażeni w przeglądarkę możemy podjąć próbę utworzenia aplikacji w AWS.



Rysunek 1.13. Środowisko Cloud9 w AWS

Dostęp do rekordów danych. Głównym problemem w większych firmach, które zaczynają korzystać z usług w chmurze, jest zapewnienie zgodności z wewnętrznymi zasadami podczas udostępnienia danych w chmurze. Zanim przeniesiemy się do chmury, musimy określić dostęp do rekordów danych oraz kroki potrzebne do jego uzyskania.

- W jaki sposób będziemy mieć dostęp do naszych danych lokalnych z poziomu chmury?
- Jakie rekordy muszą pozostać w naszej infrastrukturze?
- Czy musimy przestrzegać zasad zgodności i regulacji?
- Czy nasze dane mają format odpowiedni dla naszych potrzeb?

Migrowanie aplikacji

Zanim przeniesiemy aplikacje do chmury AWS, musimy podjąć kilka decyzji dotyczących sposobu postępowania.

Czy aplikację można przenieść do AWS i hostować w instancji EC2 bez żadnych modyfikacji?

Aplikacje z tej kategorii można przenieść do AWS jako obraz instancji EC2. Można to dość efektywnie wykonać za pomocą narzędzi do migracji serwera oraz bazy danych, opisanych w rozdziale 2. Jednakże aplikacje, które należy dostosować do chmury, będą miały inne zależności i problemy, które należy uwzględnić.

- Aplikacja przechowuje swoje dane w bazie danych. Czy baza danych pozostanie w firmie, czy zostanie przeniesiona do chmury?
- Jeśli baza danych dla aplikacji pozostanie w infrastrukturze firmy, to czy spodziewamy się problemów z opóźnieniami, które należałoby rozważyć podczas komunikacji z bazą danych?
- Czy konieczne będzie bardzo szybkie połączenie między chmurą AWS a bazą danych w infrastrukturze firmy?
- Czy istnieją problemy ze zgodnością związane z danymi aplikacji? Czy dane w spoczynku muszą być zaszyfrowane? Czy należy szyfrować komunikację z bazą danych?
- Czy użytkownicy uwierzytelniają się w aplikacji za pośrednictwem sieci korporacyjnej? Jeśli tak, to czy należy wdrożyć usługi federacyjne w AWS dla pojedynczego logowania (*Single Sign-On* — SSO)?
- Czy na serwerze aplikacji zainstalowane są lokalne zależności, które będą wpływać na działanie serwera aplikacji w chmurze AWS?
- Czy w przypadku działania w chmurze należy uwzględnić licencje systemu operacyjnego oraz aplikacji?

Czy dostawca chmury publicznej hostuje aplikację SaaS, która powinna zastąpić naszą, ponieważ okazuje się, że jest lepsza?

To może być problem polityczny. W chmurze publicznej dostępnych jest tyle aplikacji, że istnieje niemal 100% prawdopodobieństwo, że jedna z nich mogłaby zastąpić aplikację zainstalowaną obecnie w infrastrukturze firmy.

Czy aplikacja powinna pozostać zainstalowana w infrastrukturze firmy i ostatecznie wycofana z użycia?

- Aplikacja jest hostowana na przestarzałym sprzęcie, którego działanie dobiega końca.
- Aplikacja nie jest zwirtualizowana.
- Nie istnieje wsparcie dla aplikacji.
- Z aplikacji korzysta niewielu użytkowników.

Dobrze zaprojektowana platforma

Kilka lat temu w AWS pojawił się dokument zatytułowany Well-Architected Framework, ułatwiający klientom poprawne planowanie przenosin do chmury AWS. Zawiera on wskazówki dla architektów rozwiązań w chmurze, ułatwiające tworzenie bezpiecznej, odpornej i wydajnej infrastruktury hostującej aplikacje, zgodnie z najlepszymi praktykami, opracowanymi przez lata na podstawie doświadczeń wielu klientów AWS. Nadal należy samodzielnie ocenić, czy praktyki te spełniają nasze wymagania. Nie należy w ciemno stosować żadnej z najlepszych praktyk, bez zrozumienia, dlaczego zyskała sobie to miano.

Dokumentacja platformy o dobrze zaprojektowanej architekturze również porusza wiele kluczowych kwestii, dotyczących planowania takiej architektury. Warto omówić te zagadnienia z innymi kolegami zajmującymi się aspektami technicznymi w firmie; dzięki temu łatwiej podejmiemy kluczowe decyzje dotyczące infrastruktury i aplikacji hostowanych w AWS. Dokumentacja platformy znajduje się pod adresem *https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf*. Każdą aplikację, którą zamierzamy wdrożyć w AWS, należy przeanalizować pod kątem następujących pięciu zasad dobrej architektury.

Doskonałość operacyjna. Jak najlepiej opracować, wdrożyć i monitorować aplikacje w AWS, korzystając ze zautomatyzowanych procedur monitorowania wdrażania, ciągłego ulepszania oraz zautomatyzowanych rozwiązań umożliwiających powrót do działania po awarii. Do kluczowych usług AWS, z których możemy skorzystać, należą zdarzenia i alarmy CloudWatch, CloudTrail, EC2 Auto Scaling, AWS Config oraz Trusted Advisor. Więcej informacji na ten temat znajduje się w rozdziałach 5., 7. i 8.

Oto pytania dotyczące doskonałości operacyjnej, które warto sobie zadać.

- Jak poradzimy sobie z przerwami w działaniu aplikacji? Ręcznie czy automatycznie?
- Jak można przeanalizować stan aplikacji i komponentów infrastruktury hostowanych w AWS?

Bezpieczeństwo. Jak najlepiej projektować systemy, które będą działać niezawodnie i bezpiecznie, a zarazem chronić informacje klientów i rekordy danych. Do kluczowych usług AWS, z których można skorzystać, należą IAM, AWS Organizations, dzienniki

CloudWatch, zdarzenia CloudTrail, S3 i S3 Glacier oraz dzienniki przepływu VPC. Więcej informacji na ten temat znajduje się w rozdziałach 3., 6. i 7.

Oto pytania dotyczące bezpieczeństwa, które warto sobie zadać.

- Jak zarządza się poświadczeniami bezpieczeństwa i uwierzytelnianiem w AWS?
- Jak są zabezpieczone procedury automatyczne?

Niezawodność. Jak systemy i aplikacje hostowane w AWS wznawiają działanie po awarii przy zachowaniu minimalnej przerwy? Jak aplikacje mogą spełnić nasze potrzeby dotyczące eskalacji? Do kluczowych usług AWS, z których można skorzystać, należą ELB, EC2 Auto Scaling oraz alarmy CloudWatch. Więcej informacji na ten temat znajduje się w rozdziale 5.

Oto pytania dotyczące niezawodności, które warto sobie zadać.

- Jak monitorujemy zasoby hostowane w AWS?
- Jak aplikacje hostowane w AWS przystosowują się do zmian zapotrzebowania użytkowników końcowych?

Wydajność. Jak wykorzystać zasoby obliczeniowe, aby zapewnić i utrzymać wymagania aplikacji na co dzień. Czy powinniśmy zmienić nasze rozwiązanie obliczeniowe i przejść z instancji EC2 na kontenery lub model bezobsługowy? Do kluczowych usług należą EC2 Auto Scaling, woluminy EBS oraz RDS. Więcej informacji na ten temat podaję w rozdziałach 4. i 6.

Oto pytania dotyczące wydajności, które warto sobie zadać.

- Dlaczego wybraliśmy swoją bazę danych?
- Dlaczego wybraliśmy bieżącą infrastrukturę obliczeniową?

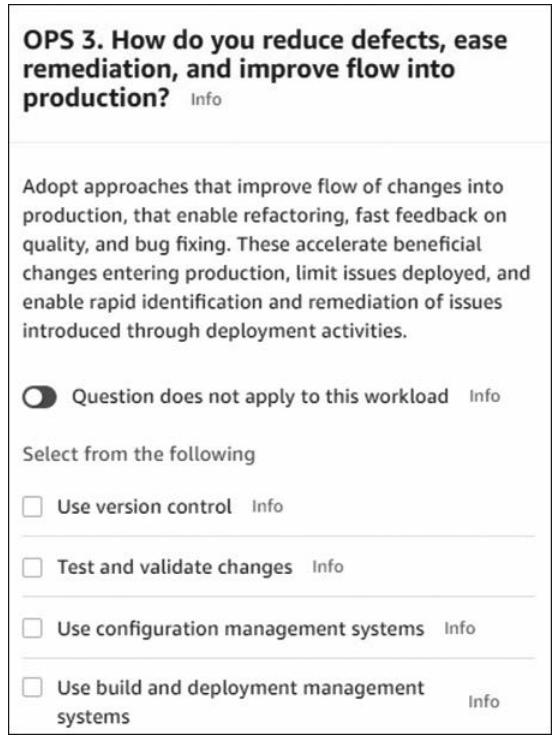
Optymalizacja kosztów. Jak projektować systemy spełniające nasze wymagania, a jednocześnie możliwie jak najtańsze? Do kluczowych usług AWS należą Cost Explorer, Budgets, EC2 Auto Scaling, Trusted Advisor oraz Simple Monthly Calculator. Więcej informacji na ten temat znajduje się w rozdziałach 2., 5. i 7.

Oto pytania dotyczące optymalizacji kosztów, które warto sobie zadać.

- Jakie wykorzystanie i koszty przewidujemy?
- Jak spełniamy cele dotyczące naszych kosztów?
- Czy znamy bieżące opłaty za transfer danych na podstawie swoich projektów AWS?

Narzędzie Well-Architected Tool

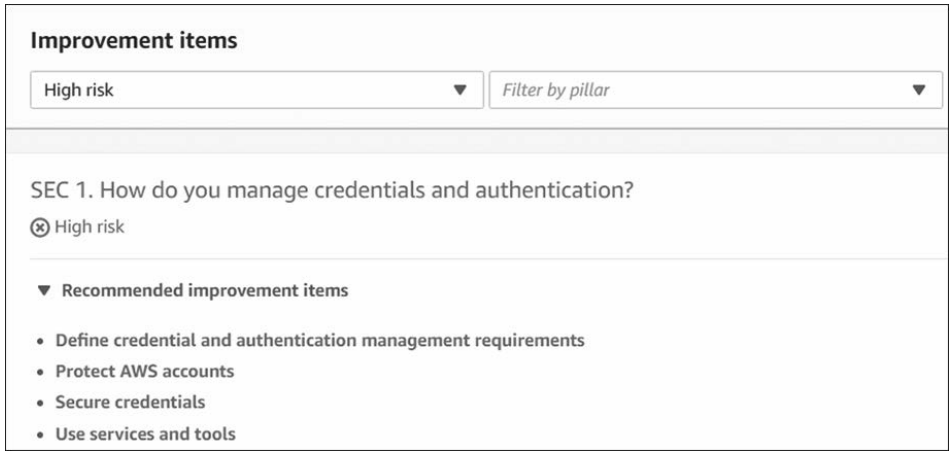
W konsoli zarządzania AWS, w sekcji „Management and Governance", dostępne jest narzędzie AWS Well-Architected Tool, widoczne na rysunku 1.14. Narzędzie to stanowi platformę służącą do sporządzania dokumentacji dotyczącej zgodności naszych procesów z najlepszymi praktykami w AWS, zdefiniowanymi w dokumentacji platformy o dobrze zaprojektowanej architekturze. Przed wdrożeniem aplikacji należy przeanalizować mnóstwo



Rysunek 1.14. Korzystanie z narzędzia Well-Architected Framework

pytań z każdego z pięciu kluczowych obszarów. W trakcie tych rozważań możemy zdefiniować kamienie milowe, które będą wyznaczać zmiany w naszej architekturze podczas cyklu wdrażania i budowania. Korzystając ze wspomnianego narzędzia i dokonując pełnego przeglądu architektury naszych aplikacji, uzyskamy wskazówki i porady dotyczące przestrzegania zalecanych przez AWS najlepszych praktyk, które powinniśmy wdrożyć. Warto poświęcić czas na analizę za pomocą tego narzędzia.

Zanim zaczniemy przegląd swojej architektury, musimy wybrać region AWS, w którym będzie hostowana nasza aplikacja. Najpierw należy zdefiniować obciążenie i wybrać branżę, a także określić, czy aplikacja znajduje się w środowisku produkcyjnym, czy przedprodukcyjnym. Podczas przeglądu narzędzie zidentyfikuje potencjalne obszary średniego i wysokiego ryzyka na podstawie informacji podanych podczas przeglądu architektury. Plan prezentujący zalecane ulepszenia w początkowym projekcie będzie też uwzględniał pięć filarów udanego projektu. Plan widoczny na rysunku 1.15 zawiera informacje o obszarach wysokiego i średniego ryzyka, a także prezentuje zalecane ulepszenia, których implementację warto rozważyć.



Rysunek 1.15. Zalecane ulepszenia po przeglądzie projektu za pomocą narzędzia Well-Architected Framework

Wnioski

W tym początkowym rozdziale opisałem współczesny krajobraz chmury publicznej oraz ustaliłem, jakie miejsce zajmuje w nim AWS z punktu widzenia infrastruktury i wdrożeń, a szczególnie z punktu widzenia rozwiązań IaaS i PaaS. Chmura jest centrum danych; nie należy tylko do nas.

W tym rozdziale napisałem też, jak instytut NIST zdefiniował chmurę publiczną oraz jak AWS pasuje do tej definicji; w większości przypadków początkowa definicja NIST przekształciła się w standard, przestrzegany przez większość korporacji, które przeniosły się do chmury AWS. Rozdział zakończyłem swego rodzaju pracą domową, sugerując rejestrację w AWS i sprawdzenie, jak można wykorzystać darmowe konto do nauki. Ponadto zachęciłem do zajrzenia na stronę AWS poświęconą zgodności, aby sprawdzić, czy wymagania dotyczące zgodności mogą zostać spełnione przez AWS. Zalecam też uważne przestudiowanie dokumentacji platformy dobrze zaprojektowanej architektury. Jest to całkiem dobry przewodnik i narzędzie online, ułatwiające zapoznanie się ze sposobem działania usług firmy Amazon oraz sugerujące sposób działania w chmurze. Platforma dobrze zaprojektowanej architektury jest też podstawą certyfikacji AWS Certified Solutions Architect – Associate, o czym warto pamiętać, jeśli w przyszłości zamierzacie zdobyć certyfikat.

Przypominam o dodatkowych filmach wideo, które są kluczowe do pracy z AWS. W dołączonych filmach prezentuję firmę Terra Firma, która będzie stadium przypadku również w tej książce. Każdy film dotyczy jakiegoś problemu lub sytuacji, z jaką mierzy się Terra Firma, a także zawiera sugerowane rozwiązanie. Również każdy rozdział rozpoczyna się od przedstawienia kilku problemów i obaw, z jakimi zmaga się Terra Firma. Mam nadzieję, że czytelnicy zrozumieją problemy firmy oraz zaprezentowane rozwiązania. Każdy rozdział kończy się kilkoma zagadnieniami do rozważenia.

> Obejrzyj film dołączony do książki, poświęcony naszemu studium przypadku: Terra Firma.

W rozdziale 2. przedstawiona zostanie szersza perspektywa, czyli regiony, strefy dostępności i lokalizacje brzegowe.

ZOSTAŃ EKSPERTEM DO SPRAW PLANOWANIA I WDRAŻANIA USŁUG AMAZON WEB SERVICES!

Przeniesienie firmowego systemu do chmury Amazon Web Services bywa sporym wyzwaniem nawet dla osób o dużej wiedzy technicznej. Wysiłek ten jest jednak uzasadniony, gdyż w chmurze AWS można korzystać ze znakomitych rozwiązań, w tym z usług obliczeniowych, magazynu, obsługi sieci i usług zarządzanych. Studiowanie dokumentacji dostępnej w internecie bywa nieefektywne i frustrujące: nader często po kilku wieczorach spędzonych na poszukiwaniach okazuje się, że odnalezione z wysiłkiem instrukcje pochodzą sprzed kilku lat i są już nieprzydatne. Brakuje również wskazówek potrzebnych przy integracji systemów, dotyczących współpracy głównych usług AWS, aspektów sieciowych, mechanizmów skalowania, zabezpieczeń i automatyzacji. Tę lukę wypełnia właśnie ta książka.

To praktyczny przewodnik dla inżynierów, którzy chcą planować i wdrażać usługi Amazon Web Services. Przyda się również osobom planującym zdobycie certyfikatu AWS. Przedstawiono tu zasady pracy zgodne z najlepszymi praktykami Well-Architected Framework firmy Amazon, wprowadzono kluczowe koncepcje, a także pieczołowicie wyjaśniono działanie i integrację głównych usług AWS. W książce znalazło się mnóstwo praktycznych, starannie przetestowanych porad dotyczących skalowalności, elastyczności i bezpieczeństwa usług obliczeniowych, magazynu, obsługi sieci oraz usług zarządzanych. Niezwykle cennym uzupełnieniem są przygotowane przez autora materiały wideo prezentujące najważniejsze koncepcje stosowane w chmurze AWS i zawierające szczegółowe instrukcje konfigurowania głównych usług AWS

W tej książce między innymi:

- rozpoczęcie pracy z Amazon Web Services
- usługi obliczeniowe oraz usługi sieciowe
- skalowalność i bezpieczeństwo aplikacji w chmurze AWS
- bezpieczeństwo przy korzystaniu z Amazon Web Services
- automatyzacja usług AWS

MARK WILKINS — jest technologiem inżynierii elektronicznej. Ma wieloletnie doświadczenie w projektowaniu, wdrażaniu i utrzymywaniu systemów IT w przedsiębiorstwach. Specjalizuje się w projektowaniu usług w chmurze z wykorzystaniem Amazon Web Services, Microsoft Azure oraz IBM Cloud. Zdobył wiele certyfikatów branżowych, prowadził także szkolenia i seminaria techniczne. Jest autorem kilku książek i licznych materiałów szkoleniowych.

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

KOD KORZYŚCI
Sięgnij po więcej!

ISBN 978-83-283-6474-5

9 788328 364745

INFORMATYKA W NAJLEPSZYM WYDANIU

Cena: 89,00 zł

Pearson
Addison-Wesley