

Mam już pięćdziesiąt lat i mogę powiedzieć, że mamy szczęście żyć w tak ciekawych technologicznie czasach. Notebook wielkości zeszytu, wykonany z tworzywa sztucznego i stopów magnezu, lżejszy niż butelka soku ma większą moc obliczeniową niż tajne rządowe centrum danych sprzed kilku dekad. Dzisiaj na jednym komputerze można uruchamiać kilka systemów operacyjnych, błyskawicznie łączyć się bezprzewodowo z mnóstwem innych urządzeń i w mgnieniu oka przysyłać komunikaty i strumienie wideo. Światłowody i radio dają dostęp do nieprzebranych ilości informacji i zasobów na całym świecie.

Urządzenia, które dzisiaj nosimy na nadgarstkach, mają miliony razy większą moc i pojemność niż jeszcze nie tak dawno stosowane komputery. To, co kiedyś zajmowało potężny budynek, było dołączone do elektrowni i obsługiwane przez setki inżynierów, dzisiaj jest niewielkim, mieszczącym się w kieszeni kawałkiem krzemu, ale mającym moc obliczeniową miliardy razy większą.

Technologia ratuje ludzkie życie, umożliwia wykonywanie operacji chirurgicznych na odległość, daje szeroki jak nigdy dotąd dostęp do informacji użytkownikom znajdującym się w powietrzu, na morzu i w każdym zakątku świata.

Kiedyś trzeba było czekać 5 – 10 minut na załadowanie programu o wielkości 48 kilobajtów, zapisanego na taśmie przesłanej pocztą. I nie była to poczta elektroniczna, tylko zwykła przesyłka dostarczana przez listonosza. Gdy pojawił się Internet, na połączenie czekało się wiele minut, a nawet godzin, ponieważ punktów dostępu było mało. Korzystało się wtedy z linii telefonicznych, numer trzeba było wykręcać lub wystukiwać na klawiaturze. Kiedy wreszcie udało się uzyskać połączenie, pozostawało jeszcze cierpliwie czekać na pobranie ogromnego, 1-megabajtowego dokumentu lub obrazu.

Tak, nie śpieszyło nam się i każdą minutę pomiędzy kolejnymi aktualizacjami mogliśmy wykorzystywać na poznawanie niuansów działania wybranego systemu operacyjnego. A dzisiaj... Dzisiaj w domu słuchamy wykładów prowadzonych na uczelni znajdującej się na innym kontynencie, a skondensowane, przyspieszone kursy informatyczne oglądamy w pociągu, w drodze do pracy lub domu. Systemy operacyjne i aplikacje są aktualizowane co 6 miesięcy, a poprawki i nowe funkcjonalności pojawiają się co tydzień. Chmura Microsoft Azure nieustannie się rozwija i w regularnych cotygodniowych odstępach wprowadza nowe funkcjonalności, aktualizacje, usługi i możliwości. Dzisiaj mamy technologii pod dostatkiem, za to brakuje nam czasu.

Wykład pierwszy, który Państwo teraz czytają w przystępny sposób opisuje najważniejsze elementy układanki o nazwie Azure i wyjaśnia wiele praktycznych pojęć, nie zajmując cennego czasu. Na początku przedstawiam modele administrowania chmurowego i filary platformy: sieci wirtualne oraz koncepcję IaaS (ang. Infrastructure as a Service — infrastruktura jako usługa).

Na temat każdej usługi i funkcjonalności Microsoft Azure można napisać osobną książkę. Materiału jest tak dużo, że każdy wykład mógłbym rozwinąć do rozmiarów książki.

Od jakiegoś czasu „chmura” jest modnym słowem, oznaczającym silny trend w branży IT. Coraz więcej firm zaczyna zmierzać w kierunku chmury. Jednak początek tej podróży

może być trudny, ponieważ potrzebne są do tego inne umiejętności i mentalność niż w przypadku lokalnej infrastruktury. Dlatego administratorzy chmurowi są bardzo poszukiwani.

Ponieważ zakładam, że zamierzają Państwo korzystać z chmury Microsoft Azure, musimy na początku poznać podstawowe pojęcia stosowane w chmurze obliczeniowej, w szczególności pojęcie chmury publicznej, jaką jest Microsoft Azure.

W branży informatycznej od samego początku jej istnienia pojawia się wiele trendów. Niektóre znikają dość szybko, inne trwają przez dłuższy czas. Wielu specjalistów uważa, że chmura obliczeniowa jest trendem, który nie będzie żył długo. Taka opinia świadczy jednak o niezrozumieniu pojęcia chmury i jego źródła.

Chmura obliczeniowa nie pojawiła się wraz z chmurą publiczną, lecz wcześniej, w latach 90. ubiegłego wieku. Oczywiście miała wtedy inną formę niż dzisiaj. Było to raczej tworzone przez firmę na własne potrzeby środowisko, w którym pracownicy mogli na żądanie tworzyć maszyny wirtualne. Taka chmura składała się z platformy wirtualizacyjnej, w której użytkownicy tworzyli własne środowiska programistyczne i testowe, gdy zachodziła taka potrzeba.

Fundament chmury obliczeniowej składa się z dwóch komponentów: platformy wirtualizacyjnej i zasobów dostępnych na żądanie. Żaden z tych komponentów nie istniałby, gdyby nie było technologii wirtualizacji, dzięki której na jednym fizycznym serwerze można tworzyć wiele maszyn wirtualnych. Chmura jest czymś więcej niż zwykłą wirtualizacją serwerów.

Możliwość uzyskiwania zasobów na żądanie jest istotą chmury obliczeniowej. Jak wspomniałem wcześniej, wszystko zaczęło się od firm budujących platformy wirtualizacyjne, na których pracownicy mogli tworzyć maszyny wirtualne na żądanie. Dzisiaj takie podejście jest nazywane chmurą prywatną.

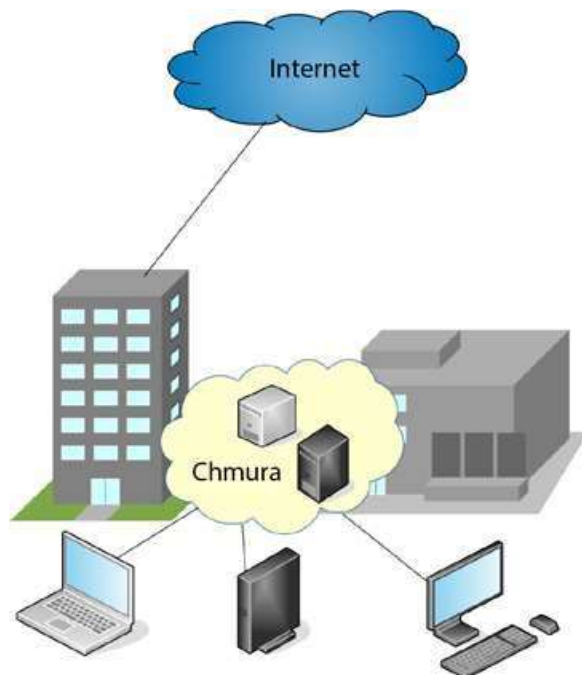
Istnieje kilka rodzajów chmur obliczeniowych. W moim odczuciu najbardziej logiczny jest podział na następujące cztery rodzaje:

- Chmura prywatna — wszystkie zasoby są utrzymywane wewnątrz we własnym centrum danych.
- Chmura hostowana — coś pomiędzy chmurą prywatną a publiczną. Dostawca usług tworzy w swoim centrum danych wydzielone, odizolowane środowisko i oferuje je klientowi na jego wyłączny użytek.
- Chmura publiczna — dostawca usług oferuje usługę publiczną, czyli dostępną dla każdego. Klienci są jednak w niej od siebie odizolowani.
- Chmura hybrydowa — połączenie chmury prywatnej i publicznej. Niektóre usługi są dostępne w chmurze prywatnej, a inne w lokalnym centrum danych. Co najmniej dwa tego rodzaju środowiska są ze sobą bezpośrednio połączone.

W chmurze prywatnej wszystkie zasoby znajdują się w lokalnym centrum danych. Aby móc z nich korzystać, nie jest potrzebny dostęp do Internetu. Komunikacja z Internetem i zasobami w chmurze przebiega osobnymi drogami, jak na poniższym schemacie. Kiedyś zbudowanie prywatnej chmury wymagało wielkich inwestycji zarówno w sprzęt, jak i w wiedzę. Przede

wszystkim potrzebne były miejsce, zasilanie i system chłodzenia. Do tego dochodziły zakupy sprzętu, np. zapór sieciowych, routerów, przełączników, serwerów, macierzy.

Dodatkowo potrzebne były licencje na platformy wirtualizacyjne, systemy operacyjne dla maszyn wirtualnych i różnego rodzaju oprogramowanie. Jednak wszystkie te inwestycje w sprzęt byłyby bezcelowe, gdyby nie było ludzi, którzy by potrafili to wszystko skonfigurować i utrzymywać przez lata. Ponadto skompletowana i działająca prywatna chmura wymagała co kilka lat kolejnych nakładów na nowe wersje oprogramowania (wirtualizacyjnego, operacyjnego) oraz na sprzęt, który trzeba było wymieniać. Zobacz poniższy rysunek:



Pojawienie się chmury hostowanej było pierwszym krokiem ku przekształceniu chmury prywatnej w publiczną. Ponieważ zbudowanie i utrzymywanie własnej chmury wymagało wielkich inwestycji, niektóre firmy wykorzystały ten fakt i zaczęły oferować usługi polegające na udostępnianiu części swoich centrów danych, z których można było korzystać jak z chmury prywatnej. Z czasem firmy te zaczęły się specjalizować w tego rodzaju działalności. Ponieważ producenci sprzętu i oprogramowania oferowali im duże upusty przy masowych zakupach, korzystanie z takich usług okazywało się korzystniejsze finansowo. W ten sposób tworzenie środowiska w chmurze hostowanej stawało się tańsze niż w prywatnej.

Do tego dochodziła kwestia początkowych inwestycji. Zbudowanie chmury prywatnej wymaga dużego początkowego nakładu finansowego na cały niezbędny sprzęt i oprogramowanie. Dlatego wiele firm decydowało się na korzystanie z chmury hostowanej, ponieważ nie wymagało to jednorazowych wydatków, lecz opłacania miesięcznej lub rocznej subskrypcji. Ponadto utrzymywanie centrum danych było prostsze, gdyż zespół ekspertów operatora mógł zajmować się środowiskami wielu klientów jednocześnie. Natomiast do obsługi jednej prywatnej chmury potrzebni byli specjaliści od sieci, macierzy, wirtualizacji itp.

W chmurze hostowanej personel techniczny też jest potrzebny, ale jeden specjalista może konfigurować, a potem utrzymywać środowiska wielu klientów. Cena za utrzymanie jest wtedy

niższa od kosztów chmury prywatnej. Natomiast niezbędny jest dostęp do chmury hostowanej w postaci sieci VPN (ang. Virtual Private Network — wirtualna sieć prywatna), połączenia lokacja – lokacja lub punkt – lokacja. Klienci uzyskują dostęp do zasobów znajdujących się poza ich własną siecią. Może to wyglądać jak na poniższym rysunku:



Kolejnym etapem chmurowej ewolucji było pojawienie się chmury publicznej. Duży dostawcy usług zaczęli oferować ogromne zasoby na żądanie. Podobnie jak w chmurze hostowanej zasoby te znajdowały się poza lokalną infrastrukturą i były obsługiwane przez firmy specjalizujące się w tej dziedzinie. Dostęp do nich był realizowany przez Internet, co pokazuje poniższy rysunek:



Pomiędzy powyższymi rodzajami chmur są dwie istotne różnice. Pierwsza polega na tym, że w chmurze hostowanej klient zazwyczaj określa z góry ilość potrzebnych zasobów i gdy chce ich dostać więcej, musi poczekać, aż zostaną skonfigurowane (o ile będzie to w ogóle możliwe). Natomiast w chmurze publicznej dostawca dysponuje ogromnymi zasobami, które udostępnia na żądanie i klient może je dostać wtedy, kiedy ich potrzebuje, w każdej ilości i w każdym rodzaju. Wystarczy, że zapłaci za subskrypcję, i od razu uzyskuje dostęp. Oznacza to również, że klient ma do dyspozycji elastycznie skalowalne środowisko i nie jest ograniczony do przyznanego mu na początku zasobów. Jeżeli na przykład utworzy maszynę wirtualną z czterema procesorami, pamięcią RAM o wielkości 16 GB, a po pewnym czasie stwierdzi, że nie jest ona w stanie podołać nałożonemu obciążeniu, nie musi tworzyć nowej maszyny — może ją powiększyć, wykorzystując opcję skalowania. Mechanizm ten działa również w odwrotnym kierunku: jeżeli okaże się, że utworzona początkowo maszyna jest za duża, klient

nie musi płacić za niepotrzebne zasoby — wystarczy, że zmniejszy maszynę, i problem rozwiązany.

Druga różnica między chmurą hostowaną a publiczną leży w opłatach. W chmurze hostowanej klient otrzymuje ustaloną ilość zasobów w zamian za miesięczną lub roczną subskrypcję, która jest stała niezależnie od tego, czy klient wykorzystuje 10% czy 100% zasobów. W chmurze publicznej opłata jest uzależniona od ilości wykorzystywanych zasobów. W tym modelu klient płaci tylko za to, z czego korzysta. Jeżeli utworzy maszynę wirtualną, płaci tylko za okres, w którym z niej korzysta. Jeżeli ją zatrzyma lub usunie, przestaje płacić. Model płatności może się różnić w zależności od dostawcy, na przykład opłata może być naliczana za każdy dzień, godzinę lub minutę użytkowania. W chmurze Microsoft Azure stosowany jest minutowy system rozliczania. Jeżeli na przykład klient utworzy maszynę wirtualną i usunie ją po 12 dniach, 11 godzinach i 13 minutach, to opłata zostanie naliczona dokładnie za ten okres. W systemie rozliczeń godzinowych opłata zostałaby naliczona za 12 dni i 12 godzin, a w przypadku rozliczeń dziennych — za 13 dni.

Kolejną różnicą jest wielopodmiotowość (ang. multitenancy). Chmura publiczna jest dostępna dla każdego. Klient, wykupując subskrypcję, tworzy własny podmiot (ang. tenant). Za pomocą specjalnego systemu zasoby przydzielone poszczególnym podmiotom są od siebie oddzielone, a zasoby przydzielone danemu podmiotowi są dostępne tylko dla jego użytkowników.

Podsumowując, najważniejsze cechy chmury publicznej to:

- ☐ dostępność przez Internet,
- ☐ wielopodmiotowość,
- ☐ zasoby dostępne na żądanie,
- ☐ płatność uzależniona od wykorzystania zasobów,
- ☐ wysoka skalowalność.

Pojęcia „chmura” lub „chmura publiczna” nie są wytworami współczesnej branży IT. Pojawiły się w latach 60. ubiegłego wieku wraz z ideą współdzielenia zasobów w czasie. Koncepcja ta przekształciła się w latach 90. w chmurę prywatną, a w znanej obecnie formie pojawiła się na początku tego stulecia. Wszystko zaczęło się od jednej ze spółek Amazona — Amazon Web Services — która w 2006 r. udostępniła usługę Elastic Cloud Compute (EC2). W ślad za nią Google zaoferował w 2008 r. usługę Google App Engine. Microsoft zapowiedział w październiku 2008 r. utworzenie własnej wersji chmury, którą publicznie udostępnił w lutym 2010 r. Potem pojawili się kolejni dostawcy własnych chmur publicznych, m.in. IBM i Oracle. Obecnie pod względem udziału w rynku i szybkości rozwoju w czołówce znajdują się tylko dwie firmy: Amazon Web Services i Microsoft.

Jak wspomniałem, Microsoft swoją wersję chmury publicznej zapowiedział w 2008 r., a udostępnił w 2010 r. W tamtym czasie oficjalna nazwa chmury brzmiała Windows Azure, ale w kwietniu 2014 r. została zmieniona na Microsoft Azure. Powód tej zmiany nie został ujawniony, ale krąży kilka domysłów. Jeden z nich głosi, że przyczyną było wykorzystanie otwartego oprogramowania. Microsoft wprowadził do oferty maszynę wirtualną z systemem Linux i nazwa chmury stała się myląca. Na początku maszyna z takim systemem nazywała się

Windows Azure Linux, jednak umieszczenie w jednej nazwie słów Windows i Linux okazało się bardzo niezręczne.

W miarę upływu lat zmieniały się nie tylko nazwy. Pierwsza wersja chmury, Windows Azure, miała zupełnie inną specyfikację niż dzisiaj. Portal też wyglądał inaczej. W pierwotnej wersji był on dostępny pod adresem <https://manage.windowsazure.net> i wykorzystywał technologię Silverlight. Był to tzw. „klasyczny” portal, a model zarządzania zasobami otrzymał nazwę Azure Standard Management (ASM). W owym czasie Microsoft znalazł błędy w swojej chmurze i rozpoczął pracę nad zupełnie nowym modelem. W 2014 r. udostępnił zmieniony portal Azure wraz z systemem zarządzania Azure Resource Manager (ARM) oferującym nowe funkcjonalności, m.in. kontrolę dostępu opartą na rolach (ang. Role-Based Access Control, RBAC) i grupowanie zasobów. Funkcjonalności te zmieniły sposób zarządzania zasobami w chmurze. W poprzednim modelu, ASM, jedynym sposobem nadania użytkownikowi uprawnień do zarządzania zasobami Azure było uczynienie go współadministratorem. Uzyskiwał on w ten sposób nieograniczony dostęp i kontrolę nad subskrybowanymi zasobami. W modelu RBAC można użytkownikom przydzielać różne poziomy uprawnień, na przykład do odczytu lub tworzenia zasobów, ale bez pełnego dostępu.

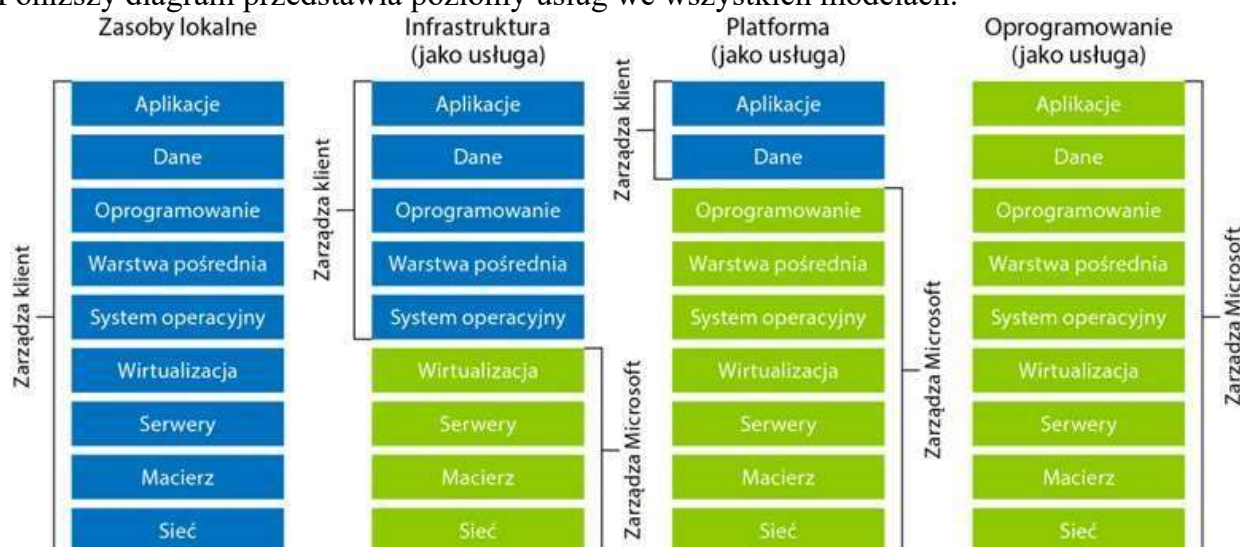
Jeszcze większym usprawnieniem było grupowanie zasobów. Grupa zasobów jest to logiczny kontener, w którym umieszcza się wybrane zasoby. Mogą ją stanowić na przykład wszystkie zasoby wykorzystywane przez daną aplikację. Użytkownik mający dostęp do takiej grupy może zarządzać tylko tymi zasobami, które się w niej znajdują. Ponadto, gdy zaloguje się do swojego podmiotu, będzie widział tylko grupę, która została mu przypisana, nawet jeżeli podmiot lub subskrypcja obejmują kilka grup. Model RBAC daje jeszcze większą kontrolę, ponieważ pozwala przypisywać użytkownikowi wybrane zasoby. Jednak jest to model zbyt szczegółowy i trudny w utrzymaniu. Dobrą praktyką i najlepszym sposobem zarządzania usługami Azure jest przypisywanie użytkownikom grup zasobów.

Za datę udostępnienia nowego portalu uznaje się grudzień 2015 r., kiedy otrzymał on adres <https://portal.azure.com>. Portal był dostępny już wcześniej, bo w kwietniu 2014 r., ale wtedy była to jego wstępna wersja. Klasyczny portal został ogłoszony jako przeznaczony do wycofania, co ostatecznie nastąpiło w styczniu 2018 r. Model ARM oprócz RBAC i grupowania zasobów zaoferował kolejną wyjątkową funkcjonalność — szablony, czyli pliki JSON zawierające informacje o zasobach. Za pomocą szablonów można rezerwować nowe zasoby lub modyfikować istniejące.

Dzięki modelowi ARM i szablonom Microsoft poszedł mocno do przodu i znacząco zmienił branżę chmurową. W chmurze i metodyce DevOps bardzo ważne jest pojęcie IaC (ang. Infrastructure as Code — infrastruktura jako kod), a szablony idealnie się w nie wpisują. Za pomocą raz przygotowanego szablonu można powielać środowiska. Automatyzuje się w ten sposób proces wdrażania i konfigurowania infrastruktury, unikając przy tym błędów. Z pojęciem IaC związanych jest wiele terminów chmurowych. Najważniejsze rodzaje usług w chmurze Microsoft Azure (i w chmurze w ogólności) to:

- IaaS (ang. Infrastructure as a Service — infrastruktura jako usługa),
- PaaS (ang. Platform as a Service — platforma jako usługa),
- SaaS (ang. Software as a Service — oprogramowanie jako usługa).

Każdy z tych modeli reprezentuje inny poziom usług i sposób kontroli zasobów. Aby wyjaśnić relacje między nimi, najlepiej jest porównać je z usługami w lokalnym centrum danych. Poniższy diagram przedstawia poziomy usług we wszystkich modelach:



W lokalnym centrum danych użytkownik jest odpowiedzialny za skonfigurowanie i utrzymanie całej infrastruktury. Musi przygotować sieć i macierze, zakupić i skonfigurować sprzęt, zainstalować oprogramowanie, uruchomić serwer wirtualizacyjny. Następnie musi utworzyć obrazy maszyn i zainstalować bazy danych. Jego zadaniem jest również dbanie o bezpieczeństwo w całym zakresie, począwszy od ochrony fizycznej, poprzez zabezpieczenie sieci, serwerów i systemów operacyjnych, aż po całe oprogramowanie aplikacyjne działające na serwerach. W modelu IaaS jest łatwiej. Klient nie musi niczego przygotowywać. Wystarczy jedynie, że wykupi subskrypcję i utworzy maszynę wirtualną, z której może zacząć korzystać, gdy będzie mu potrzebna. Zakup, przygotowanie, konfiguracja i utrzymanie infrastruktury nie są już jego problemem, ponieważ zajmuje się tym dostawca usług, w naszym przypadku Microsoft. Klient nie musi też przygotowywać ani wdrażać obrazów maszyn. Zapewnienie bezpieczeństwa także jest prostsze, gdyż za ochronę sprzętu, sieci i serwerów jest odpowiedzialny Microsoft. W kwestii bezpieczeństwa zadaniem klienta jest aktualizowanie systemów oraz instalowanie poprawek i zabezpieczeń. Do jego zadań należy też ochrona aplikacji, dlatego aby to robił dobrze, musi znać najlepsze praktyki w tym zakresie. Wielu klientów zapomina, że migrując infrastrukturę do chmury, muszą wzmocnić jej ochronę. Ponieważ bezpieczeństwem w dużej mierze zajmuje się dostawca usług, wielu klientów uznaje, że mogą się odprężyć i darować sobie dbanie o nie w zakresie, który do nich należy. Przechodząc do chmury, trzeba pamiętać, że zasoby i aplikacje są wystawiane na widok publiczny i częściej niż w przypadku infrastruktury lokalnej stają się obiektami ataków. Aby haker mógł zaatakować lokalne zasoby, musi się przedostać przez zaporę sieciową, włamać do serwera i pozyskać dane. W chmurze wiele usług jest dostępnych przez Internet, dlatego jeszcze staranniej trzeba dbać o ich bezpieczeństwo. Najlepszym przykładem modelu IaaS w chmurze Microsoft Azure jest maszyna wirtualna z systemem Windows lub Linux. Co ciekawe, jak podaje Microsoft, w październiku 2017 r. ponad 40% maszyn wirtualnych w chmurze Azure wykorzystywało system Linux. Model PaaS jest jeszcze prostszy w użyciu niż IaaS. Dostawca usług troszczy się o wszystko, o czym napisałem wyżej, i o jeszcze więcej. Microsoft zajmuje się systemem operacyjnym, niezbędnym dodatkowym oprogramowaniem i dodatkowymi

zabezpieczeniami. Użytkownik musi zadbać o resztę (zależną od usługi PaaS) i po części o bezpieczeństwo (o którym często zapomina, jak w poprzednim modelu, ponieważ Microsoft przejmuje jeszcze więcej obowiązków). W modelu IaaS wykorzystywane są sieci VPN lub połączenia typu punkt – lokacja i lokacja – lokacja. W takim wariantcie punkty dostępu nie są upubliczniane. W modelu PaaS jest inaczej, wykorzystywany jest bowiem głównie dostęp przez Internet. Z tego powodu bezpieczeństwo należy traktować bardzo poważnie. Zaniedbania grożą utratą danych i niezamierzonym udostępnieniem usług. Przykładami modelu PaaS w chmurze Azure są usługi Azure App Service i Azure SQL Database. Ostatnim modelem jest SaaS. W tym przypadku dostawca usług troszczy się niemal o wszystko, od początku do końca. Klient otrzymuje gotowe rozwiązanie i jego jedynym obowiązkiem jest wykupienie subskrypcji i nadanie swoim użytkownikom odpowiednich uprawnień dostępu. Zazwyczaj w modelu SaaS wyróżniane są moduły administratora i użytkownika. Pierwszy jest stosowany do zarządzania kontami użytkowników i poziomami dostępu. Natomiast moduł użytkownika umożliwia korzystanie z subskrybowanych funkcjonalności. Domeną klienta jest również bezpieczeństwo, ale tylko na poziomie użytkownika. Musi on zadbać o to, aby użytkownicy przechowywali swoje poświadczenia w bezpiecznych miejscach, definiowali odpowiednio silne hasła chroniące przed tzw. atakami brutalnej siły. Przykładem modelu SaaS w chmurze Azure jest Microsoft 365. Do pokazania, jak usługi chmurowe odnoszą się do rzeczywistości, i do lepszego wyjaśnienia, czym jest chmura obliczeniowa, często wykorzystywany jest poniższy diagram modelu „pizza jako usługa”, gdzie pizza jest porównana z opisanymi wcześniej modelami IaaS, PaaS i SaaS oraz z lokalnym centrum danych. Analogią do korzystania z lokalnego centrum danych jest przygotowywanie pizzy w domu. Trzeba kupić wszystkie składniki, wymieszać je, upiec, kupić napoje i podać. Odpowiednikiem usługi IaaS jest zakup mrożonej pizzy, upieczenie jej, przygotowanie nakrycia i podanie. Z kolei usługę PaaS można porównać z zamówieniem pizzy z dostawą. W tym przypadku wystarczy jedynie kupić napoje i podać pizzę. Wreszcie równoważnikiem usługi SaaS jest wizyta w pizzerii: wchodzimy, zamawiamy wszystko, czego potrzebujemy, a obsługa robi wszystko za nas, czyli przygotowuje pizzę, podaje napoje itd. Opisałem już kilka funkcjonalności i zalet poszczególnych modeli usług chmurowych. IaaS wymaga większego zaangażowania klienta niż PaaS. Najłatwiej jest w przypadku modelu SaaS, w którym udział klienta jest najmniejszy, a utrzymywanie infrastruktury polega jedynie na zarządzaniu kontami użytkowników.

Pizza jako usługa

Model tradycyjny (lokalny)	Infrastruktura jako usługa (IaaS)	Platforma jako usługa (PaaS)	Oprogramowanie jako usługa (SaaS)
Stół	Stół	Stół	Stół
Napoje	Napoje	Napoje	Napoje
Prąd/gaz	Prąd/gaz	Prąd/gaz	Prąd/gaz
Piec	Piec	Piec	Piec
Ciepło	Ciepło	Ciepło	Ciepło
Ciasto	Ciasto	Ciasto	Ciasto
Ketchup	Ketchup	Ketchup	Ketchup
Dodatki	Dodatki	Dodatki	Dodatki
Ser	Ser	Ser	Ser
Przygotowana w domu	Kupiona w supermarkecie	Na zamówienie	W pizzerii

Zarządza konsument
 Zarządza producent

Jest jednak druga strona medalu. Utrzymanie infrastruktury i administrowanie nią w modelu SaaS wymaga minimalnego zaangażowania, ale możliwości jej dostosowywania też są minimalne. Aby w niej coś zmienić, trzeba się kontaktować z dostawcą usługi, bo tylko on może wprowadzać modyfikacje.

PaaS daje większą swobodę pod względem administrowania, utrzymywania i dostosowywania infrastruktury. Zazwyczaj jednak zmiany ograniczają się do określonych ustalonych opcji konfiguracyjnych, ale to i tak więcej niż w przypadku modelu SaaS.

IaaS wymaga największego zaangażowania klienta w administrowanie infrastrukturą i jej utrzymanie, ale też oferuje największe możliwości konfiguracyjne. Klient ma kontrolę nad wszystkim, co znajduje się na poziomie systemu operacyjnego i wyżej (może wybierać różne przygotowane wcześniej obrazy systemów, a nawet tworzyć własne). Może wybierać funkcjonalności, które zamierza konfigurować, zarządzać rolami użytkowników na serwerach i instalować na maszynach wirtualnych dowolne oprogramowanie.

Przy wyborze modelu kluczową kwestią jest uświadomienie sobie, jakie funkcjonalności są najbardziej dopasowane do potrzeb w danej sytuacji. Czasami, gdy produkt oferuje wszystko, co trzeba, najprostszym rozwiązaniem jest wybranie modelu SaaS. Jeżeli niezbędne są najnowsze ustawienia i funkcjonalności, prawdopodobnie najlepszy będzie PaaS. Jeżeli natomiast wymagane są nietypowe rozwiązania, wtedy właściwym wyborem będzie IaaS, ponieważ w tym modelu można skonfigurować i zainstalować wszystko, co jest potrzebne do uruchomienia aplikacji.

Podstawową zaletą chmury obliczeniowej we wszystkich opisanych modelach jest łatwość utrzymywania infrastruktury i zarządzania nią.

W dziedzinie usług chmurowych istnieje wiele obszarów specjalistycznej wiedzy, której klient nie musi posiadać, ponieważ ma ją dostawca usług. Tutaj kryje się jednak pewna pułapka. Zasoby w chmurze nie obsługują się same. Do tego potrzebni są specjaliści, którzy zarządzają zasobami i utrzymują je w należytym stanie. Wymagana jest przy tym inna wiedza niż w przypadku lokalnych centrów danych, ale podstawy informatyki też są potrzebne. W przypadku modelu IaaS niezbędny jest administrator systemu operacyjnego Windows (lub Linux, w zależności od preferencji). Jeżeli wykorzystywane są bazy danych, potrzebny jest ich administrator. Specjaliści IT muszą poszerzać swoje umiejętności odpowiednio do ról pełnionych w chmurowym środowisku. Mogą wprowadzić zapomnienie o lokalnej infrastrukturze, ale wciąż są bardzo potrzebni.

Jedną z największych zalet chmury są korzyści finansowe. W przypadku lokalnego środowiska trzeba samodzielnie kupować wszystkie zasoby i płacić za nie z góry, jeszcze zanim zaczną się z nich korzystać. Aby utworzyć lokalne centrum danych, trzeba przygotować wiele komponentów, takich jak zapory sieciowe, przełączniki, macierze, serwery, systemy zasilania itp. Do tego potrzebne są warunki umożliwiające korzystanie z tego sprzętu, m.in. odpowiednie pomieszczenia. Niezbędne są systemy chłodzenia, które będą utrzymywać urządzenia w odpowiedniej temperaturze, oraz systemy zasilania, które zapewnią wymaganą moc bez przeciążania sieci elektrycznej. Gdy wszystko już będzie na miejscu, trzeba kupić licencje dla serwerów wirtualizacyjnych, dla systemów operacyjnych wszystkich maszyn wirtualnych oraz dla całego oprogramowania, na przykład baz danych czy programów antywirusowych. To wszystko trzeba najpierw kupić i skonfigurować, co dla niejednej firmy może być poważnym wyzwaniem finansowym.

Po poniesieniu początkowych kosztów trzeba płacić za utrzymanie całości, czyli za prąd, system chłodzenia i części zamienne. Dodatkowo potrzebny jest ktoś, kto będzie to wszystko robił.

Po kilku latach sprzęt i oprogramowanie zestarzeją się i trzeba będzie wszystko robić od nowa. Nierzadko trudno jest utrzymać tempo w takich warunkach.

W chmurze nie trzeba płacić za nic z góry. Opłaty za usługi są pobierane zgodnie z modelem „płać za to, czego używasz”, czyli za zasoby wykorzystywane w każdej minucie. Nie ponosi się żadnych dużych wydatków, ponieważ zasoby rezerwuje się wtedy, gdy są potrzebne, i na wymagany okres. Kiedy przestaną być potrzebne, można je zwolnić.

Jeżeli potrzebny jest nowy serwer, w chmurze można go utworzyć w kilka minut. Nie trzeba w tym celu kontaktować się z dostawcą, składać zamówienia i czekać na dostawę. W chmurze Azure nową maszynę wirtualną (lub dowolny inny zasób) uruchamia się wtedy, gdy jest ona potrzebna. Kiedy przestanie się z niej korzystać, można ją usunąć w jednej chwili, dzięki czemu nie trzeba za nią płacić. To także jest jedna z zalet odróżniających chmurę od lokalnej infrastruktury: kupowane zasoby nie są ciężarem. Aby móc korzystać z zasobów w lokalnym centrum danych, trzeba je najpierw kupić. Jednak gdy przestaną być potrzebne, nie znikają w magiczny sposób i nie można odzyskać zainwestowanych pieniędzy.

Nie lada wyzwaniem może być określenie ilości potrzebnych zasobów. Załóżmy, że tworzymy nową aplikację WWW, z której będą korzystali zewnętrzni użytkownicy. Aplikacja jest już gotowa i trzeba ją gdzieś uruchomić, aby użytkownicy mogli założyć konta i zacząć z niej korzystać. Potrzebny jest system operacyjny, serwer WWW i baza danych. Trzeba dla nich kupić licencje. Problem polega na tym, że niezbędny jest odpowiednio wydajny sprzęt. Oszacowanie początkowego obciążenia wprowadzanego przez użytkowników, a potem tempa jego wzrostu może być bardzo trudne. Łatwo jest popełnić błąd w szacunkach. Jeżeli je zawyżymy, zapłacimy za zasoby, które nie będą wykorzystywane. Jeżeli zaniżymy, wkrótce potrzebna będzie rozbudowa infrastruktury. Pojawia się wtedy dwa problemy: czas i pieniądze. Rozbudowa sprzętu zajmuje jakiś czas. Gdy będziemy czekać na dostawę komponentów, użytkownicy będą doświadczać problemów wynikających z przeciążenia serwerów. Utrata użytkowników zniechęconych niską wydajnością aplikacji jest czymś, czego zdecydowanie chcielibyśmy uniknąć, ale nie będziemy w stanie temu zaradzić, ponieważ uzyskanie zgody na zakup niezbędnych komponentów oraz ich dostawa i instalacja trwają dłuższą chwilę (szczególnie w dużych firmach). Ponadto na czas instalacji nowych komponentów trzeba wyłączyć wszystkie serwery, czego też nie chcemy robić.

Kolejną kwestią rozbudowy są jej koszty. Zwiększenie wydajności serwerów może kosztować sporo pieniędzy. Czasami aby rozszerzyć pamięć, trzeba najpierw wymienić procesor, co z kolei może wymagać uprzedniej wymiany płyty głównej. Zdarza się, że możliwości rozbudowy są ograniczone i nie można nic zrobić. W takiej sytuacji trzeba kupić nowy sprzęt. Starego serwera nie będziemy już używać, mimo że za niego zapłaciliśmy.

W chmurze wszystkie te problemy są o wiele prostsze. Wystarczy utworzyć drugi serwer (w modelu IaaS) lub drugą usługę (w modelu PaaS). Są też inne opcje. Zarządzanie obciążeniem i zasobami jest łatwe, szybkie i przyjemne.

Jeżeli po pewnym czasie okaże się, że zasoby zostały przeszacowane, można je po prostu ograniczyć i problem rozwiązany. Klient nie jest skazany na coś, czego nie potrzebuje, i nie musi za to płacić. Kilka chwil po zmniejszeniu mocy serwera lub ilości zasobów klient płaci mniej — tylko za to, czego aktualnie potrzebuje.

Jeśli natomiast zasoby okażą się niedoszacowane, można je równie szybko i łatwo rozszerzyć. Nie trzeba tracić czasu, czekając na komponenty. Wystarczy po prostu rozszerzyć zasoby i problem rozwiązany.

Kolejna zaleta chmury to ilość zasobów. Czasami zdarzają się gwałtowne skoki intensywności wykorzystania aplikacji. Obciążenie zasobów, spodziewane lub nie, gwałtownie rośnie. Na przykład można przewidzieć wzrost odwiedzin sklepu internetowego przed świętami lub w okresie posezonowej wyprzedaży. Portal informacyjny też może być poddany większemu obciążeniu, na przykład gdy pojawi się ważna wiadomość.

Przygotowując potrzebne zasoby, uwzględnia się przewidywane i nieprzewidywane wzrosty obciążenia. Trzeba wtedy nabyć odpowiedni sprzęt, nawet jeżeli przez większość czasu będzie on wykorzystywany w niewielkim stopniu. Jeżeli w ciągu zwykłego dnia z aplikacji korzysta 10 000 użytkowników, a w szczycie będzie ich 1 000 000, trzeba przygotować zasoby, które obsłużą taką liczbę. W przeciwnym wypadku aplikacja zostanie przeciążona i przestanie

reagować na działania użytkowników, których firma w efekcie straci. Jednak zakup serwera, który przez 90% czasu nie będzie w pełni wykorzystywany, to wydatek, którego chcielibyśmy uniknąć. Pojawia się wybór: zapłacić więcej czy stracić klientów.

Dzięki chmurze z tym problemem też można poradzić sobie bardzo łatwo. Zasoby można zwiększać i zmniejszać łatwo i szybko. W zależności od tego, czy wzrosty obciążenia można przewidzieć, czy nie, stosuje się jedną z dwóch strategii.

W przypadku nieprzewidzianego wzrostu można zwiększać lub zmniejszać ilość zasobów na żądanie. Dzięki temu nie trzeba płacić za duże zasoby, które pozostają niewykorzystane poza okresem, kiedy są rzeczywiście potrzebne. Przy zwykłym obciążeniu klient płaci za niewielką ilość zasobów, a w okresie szczytu za większą, ale tylko do czasu, aż obciążenie spadnie do zwykłego poziomu.

Jeżeli wzrosty obciążenia są nieprzewidywalne, można skonfigurować wskaźniki wydajności i alarmy, które będą skutkować rozszerzeniem lub ograniczeniem zasobów. Na przykład może to być wskaźnik obciążenia procesora, który po przekroczeniu 90% automatycznie zwiększy ilość zasobów przydzielonych określonej usłudze. Dzięki temu nie pojawią się problemy wynikające ze zwiększonego obciążenia aplikacji. Mechanizm automatycznego skalowania zasobów trzeba konfigurować ostrożnie, ponieważ jeżeli nie będzie ograniczał zasobów, naliczane będą wysokie opłaty. Zasoby można ograniczać ręcznie lub automatycznie. Można na przykład skonfigurować drugi wskaźnik, który będzie zmniejszał ilość zasobów, gdy obciążenie procesora spadnie poniżej 50%. W ten sposób klient będzie miał do dyspozycji ilość zasobów odpowiednią do potrzeb.

Modele subskrypcji u większości dostawców są do siebie podobne i różnią się jedynie pewnymi unikatowymi szczegółami. Skupmy się na chmurze Microsoft Azure, ponieważ jej poświęcona jest ta książka. Wszystkie opisane dalej funkcjonalności będą dotyczyły tej platformy.

Najwyższą jednostką administracyjną w chmurze Azure jest podmiot. Azure jest chmurą publiczną, w której większość centrów danych jest dostępna dla każdego klienta na całym świecie. Są jednak wyjątki. Na przykład amerykańskie centrum rządowe jest dostępne tylko dla instytucji podległych rządowi Stanów Zjednoczonych. Chińskie centrum obsługuje tylko instytucje publiczne w Chinach, a centrum niemieckie tylko firmy zarejestrowane w Niemczech.

Microsoft jest publicznym dostawcą usług i przechowywane przezeń dane poszczególnych klientów muszą być od siebie odizolowane. Do tego celu wykorzystywana jest usługa Azure Fabric. Mimo że klienci używają tych samych fizycznych zasobów, takich jak sieć, serwery i macierze, usługi są dostępne tylko dla ich właścicieli.

Podmiot jest tworzony w momencie wykupienia subskrypcji. Wielu klientów, na przykład korzystających z usługi Microsoft 365, nawet nie wie, że są podmiotami w chmurze Azure. Usługa Microsoft 365 wymaga dostępności usługi Azure Active Directory i tworzy pierwszy podmiot. Spotkałem wielu klientów, którzy niepotrzebnie tworzyli nowy podmiot, choć używali już Microsoft 365. Rzecz w tym, że podmiot jest powiązany z usługą Azure Active Directory i utworzenie nowego podmiotu skutkuje uruchomieniem kolejnej usługi. W miarę

upływu czasu, gdy obie usługi coraz bardziej zaczynają się od siebie różnić, zarządzanie nimi staje się coraz trudniejsze.

Wraz z wykupieniem pierwszej subskrypcji tworzone są nowy podmiot i nowa usługa Azure Active Directory. Można nią zarządzać na kilka sposobów, które przedstawię w kolejnych wykładach. Uruchomienie nowej usługi Azure Active Directory też skutkuje utworzeniem nowego podmiotu.

Poziom niżej od podmiotu znajduje się subskrypcja. Z jednym podmiotem może być skojarzonych wiele subskrypcji. Nowo utworzony podmiot zawiera tylko usługę Azure Active Directory, bez subskrypcji. Ponieważ usługa ta składa się z wielu warstw, bez aktywnej subskrypcji nie można zmienić jej wariantu na przykład z podstawowego (Basic) na inny. Subskrypcja jest niezbędna do zbierania informacji o wykorzystaniu zasobów, generowania raportów i otrzymywania faktur za korzystanie z usługi.

Jeżeli korzysta się z wielu środowisk, można je ze względów finansowych lub administracyjnych subskrybować oddzielnie. Robi się to na wiele sposobów w zależności od potrzeb. Można na przykład posiadać jeden podmiot odpowiadający firmie i subskrypcje dla poszczególnych działów. Do każdej subskrypcji można przypisać innego administratora i w ten sposób kontrolować koszty generowane przez poszczególne działy. Innym przykładem separacji subskrypcji jest posiadanie kilku środowisk przeznaczonych do różnych celów. Miałem do czynienia z wieloma firmami, które wykupiły osobne subskrypcje dla środowisk programistycznego, testowego i produkcyjnego. Firma mogła zarządzać każdym środowiskiem niezależnie i kontrolować koszty generowane przez każde z nich.

Kolejnym poziomem w hierarchii są grupy zasobów. Funkcjonalność ta, wprowadzona w modelu ARM, ma wiele zalet. Podobnie jak w przypadku subskrypcji, zasoby można łączyć w grupy według kryteriów logicznych i finansowych. Na przykład można tworzyć osobne grupy dla poszczególnych działów firmy lub środowisk (programistycznego, testowego, produkcyjnego). Do każdej grupy można przypisać osobnego administratora, który będzie kontrolował ponoszone wydatki. Należy pamiętać, że za wszystkie usługi wystawiana jest na koniec miesiąca tylko jedna faktura, dlatego koszty związane z poszczególnymi grupami trzeba kontrolować samodzielnie. O wiele łatwiej jest rozdzielać rozliczenia na poziomie subskrypcji. Jeżeli potrzebne są osobne faktury dla każdego działu lub środowiska, należy wykupić osobne subskrypcje.

Wszystkie sposoby dostępne w chmurze Azure tworzą hierarchiczną strukturę. Zasoby należą do grup, grupy do subskrypcji, a subskrypcje do podmiotu. Użytkownik po zalogowaniu się do portalu ma dostęp do domyślnego podmiotu. Z jednym kontem może być skojarzonych wiele podmiotów, dlatego istnieje możliwość określenia, który z nich ma być podmiotem domyślnym. Na przykład w moim firmowym koncie domyślnie wybrany jest podmiot przypisany mojej firmie. Jednak mam gościnny dostęp do podmiotów moich klientów. Domyślnie po zalogowaniu łączę się z własnym podmiotem, ale z rozwijanej listy mogę wybrać inny. Mogę również wskazać inny podmiot jako domyślny, z którym będę się łączył po zalogowaniu do konta.

Z perspektywy Microsoft Azure, gdy użytkownik zaloguje się do swojego konta, usługa Azure Fabric określa, do których podmiotów ma on dostęp, i łączy go z domyślnym podmiotem. Użytkownik uzyskuje wtedy dostęp do subskrypcji i zasobów przypisanych temu podmiotowi i może nimi zarządzać. Przełączając się pomiędzy podmiotami, użytkownik uzyskuje dostęp do innych subskrypcji i grup zasobów. Cały proces jest kontrolowany przez Azure Fabric, aby środowiska różnych klientów były od siebie odizolowane.

W podobny hierarchiczny sposób można administrować zasobami. Użytkownik może posiadać różnego rodzaju uprawnienia dostępu do zasobów, na przykład jako właściciel, udziałowiec, odbiorca itp. Za pomocą ról i polityk można definiować niestandardowe uprawnienia. Role użytkowników mogą dotyczyć podmiotu, grupy zasobów lub pojedynczego zasobu. Zarządzanie uprawnieniami użytkowników na poziomie zasobów jest trudne i czasochłonne, dlatego nie jest zalecane.

Z drugiej strony należy unikać przydzielania dostępu na poziomie podmiotu, ponieważ udostępnianie użytkownikom wszystkich zasobów może nie być pożądane. Wyjątkiem może być mała grupa administratorów, ale takiego podejścia również nie należy stosować. Najlepszą i najczęściej używaną opcją jest przydzielanie dostępu użytkownikom na poziomie subskrypcji lub grup zasobów. Pierwszą stosuje się w przypadku, gdy wykupione są osobne subskrypcje na działy lub środowiska. Administrator może wówczas dodatkowo zarządzać subskrypcją. Drugą opcję wykorzystuje się, gdy w grupie zasobów znajduje się jedna aplikacja lub jedno środowisko. Administratorowi można powierzyć zarządzanie grupą zasobów. Nie są to jedyne możliwe opcje i modele. Można tworzyć własne lub dostosowywać istniejące odpowiednio do potrzeb. Miałem do czynienia z firmami, w których grupy zawierały podobne do siebie zasoby, przypisane administratorom za pomocą ról. Na przykład w jednej grupie umieszczone były wszystkie zasoby sieciowe przypisane inżynierom sieciowym. W osobnej grupie były bazy danych przydzielone innemu administratorowi itd.

Do skonfigurowania subskrypcji Azure potrzebnych jest kilka rzeczy. Pierwszą jest adres e-mail. Musi to być adres wykorzystywany w usłudze Microsoft Live lub Microsoft 365. Ponadto wymagane są numer telefonu, dane karty płatniczej i adres do rozliczeń. Dane karty są potrzebne również w przypadku bezpłatnych subskrypcji, ponieważ Microsoft wykorzystuje je do weryfikowania tożsamości klienta.

Istnieją trzy rodzaje subskrypcji usług Azure:

- ☐ sponsorowana,
- ☐ proporcjonalna do użycia (ang. pay as you go),
- ☐ firmowa.

Subskrypcja sponsorowana ma kilka odmian. Są to m.in. subskrypcja próbna, karta Azure, subskrypcja MSDN i sponsoring Azure. Wspólną cechą wszystkich odmian jest możliwość korzystania z określonych zasobów za darmo. Ponadto w ramach tych subskrypcji w niektórych regionach nie można korzystać z niektórych usług. Na przykład standardowe maszyny wirtualne A2 można tworzyć tylko w północnej Europie.

W ramach subskrypcji testowej użytkownik otrzymuje 200 USD o wykorzystania przez 30 dni. Subskrypcja wygasa po wyczerpaniu tej kwoty lub upływie zadanego czasu, w zależności od tego, co nastąpi wcześniej. Aby uzyskać tę subskrypcję, należy podać dane karty płatniczej. W każdej chwili subskrypcję testową można przekształcić w proporcjonalną do użycia, wykorzystując dane istniejącej lub nowej karty. Informacje te są wykorzystywane jedynie w celu weryfikacji użytkownika. Karta nie jest obciążana, dopóki użytkownik nie zdecyduje się na zniesienie limitu i rozpoczęcie płatności po upływie okresu testowego. Microsoft w ten sposób chroni chmurę Azure przed nielegalnym użyciem. Gdyby dane karty płatniczej nie były wymagane, każdy użytkownik mógłby uzyskać próbną subskrypcję i przez 30 dni wykorzystywać ją do nielegalnych celów. Po upływie okresu próbnego taka osoba mogłaby uzyskać kolejną testową subskrypcję i kontynuować nielegalną działalność. Microsoft nie byłby w stanie identyfikować takich delikwentów i sam odpowiadałby przed wymiarem sprawiedliwości za łamanie prawa.

Karta Azure jest inną odmianą testowej subskrypcji, w ramach której określona kwota jest przydzielana na okres 30 dni. Odmiana ta obejmuje oficjalne materiały edukacyjne Microsoftu, a kwota jest uzależniona od rodzaju tych materiałów, ponieważ każdy ma inną cenę. W tej odmianie subskrypcji nie jest wymagane podawanie danych karty płatniczej, gdyż użytkownik musi wcześniej zarejestrować się na wybrane szkolenie. Informacje podane podczas rejestracji są wykorzystywane do zweryfikowania użytkownika. Podobnie jak w przypadku subskrypcji testowej użytkownik uzyskuje dostęp do ograniczonych rodzajów i ilości zasobów w niektórych regionach. Subskrypcja MSDN Azure jest powiązana z subskrypcją MSDN. Kwota również jest uzależniona od poziomu subskrypcji MSDN (profesjonalnej lub firmowej) i jest przydzielana co miesiąc na początku okresu rozliczeniowego. Okres rozliczeniowy jest uzależniony od daty aktywacji. Rozpoczyna się wraz z tą datą i obejmuje 30 dni. Subskrypcja MSDN Azure jest aktywna dopóty, dopóki jest aktywna subskrypcja MSDN. Karta płatnicza nie jest potrzebna, ponieważ do weryfikacji użytkownika wykorzystywane są inne dane (płatność za subskrypcję MSDN). Jeżeli w ciągu 30 dni zostanie wyczerpana przyznana kwota, zasoby są dezaktywowane i blokowane do dnia rozpoczęcia kolejnego okresu rozliczeniowego. Aby kontynuować korzystanie z usług, trzeba poczekać do następnego okresu lub podać dane karty płatniczej, która zostanie obciążona kwotą za wykorzystanie zasobów ponad ustalony limit. Limit ten można usunąć dla jednego okresu rozliczeniowego lub dla całej subskrypcji. W pierwszym przypadku karta zostanie obciążona tylko raz w danym okresie. Jeżeli w kolejnym okresie zostanie osiągnięty limit, zasoby będą zablokowane. Natomiast w drugim przypadku karta będzie obciążana automatycznie w każdym okresie, w którym zostanie przekroczony limit.

Należy zwrócić uwagę, że w każdej z opisanych wyżej odmian subskrypcji najpierw wydawana jest sponsorowana kwota, a dopiero potem obciążana karta płatnicza. Subskrypcja MSDN jest przeznaczona tylko do celów programistycznych i testowych. Nie można jej wykorzystywać komercyjnie lub w środowiskach produkcyjnych. Ilość dostępnych zasobów i dostęp do niektórych zasobów również są ograniczone. W ramach subskrypcji MSDN za zasoby są pobierane inne opłaty. Użytkownik nie jest obciążany kosztami licencji na oprogramowanie, ponieważ wykorzystuje środowisko programistyczne lub testowe, w którym zasoby są znacznie tańsze.

Sponsoring Azure jest bardzo podobny do subskrypcji MSDN. Nie można go wykorzystywać do celów komercyjnych ani w środowiskach produkcyjnych. Kwota również jest ograniczona, z tą jednak różnicą, że okresem rozliczeniowym nie jest miesiąc, lecz rok. Jest to jedna z dwóch różnic między powyższymi odmianami subskrypcji. Limit można znieść. Dostęp do niektórych zasobów i regionów jest ograniczony. Druga różnica polega na tym, że zasoby mają zwykłe ceny i pobierane są opłaty za licencje.

Subskrypcja proporcjonalna do użycia jest najprostsza i najpopularniejsza. Aby ją wykupić, należy podać dane karty płatniczej, która będzie co miesiąc obciążana. Nazwa subskrypcji mówi sama za siebie: nie ma ograniczeń w dostępie do zasobów, a użytkownik jest obciążany tylko za to, czego używa. Jeżeli nie wykorzystuje żadnych zasobów, Microsoft nie pobiera opłat. Jeżeli zwiększy ilość zasobów, zostanie dodatkowo obciążony. Po rezygnacji z części zasobów będzie płacił tylko za te, które mu pozostały. Nie ma górnego ani dolnego limitu subskrypcji. Klient może nie płacić nic, jak również może płacić miliony.

Subskrypcja firmowa wymaga zawarcia umowy określającej minimalną kwotę, jaką użytkownik będzie w ciągu roku płacił za zasoby Azure. W zamian uzyskuje określony rabat. Opłata określona w umowie jest pobierana co miesiąc, natomiast opłata za wykorzystane dodatkowe zasoby jest pobierana na koniec roku. W ramach tej subskrypcji można również korzystać z własnych licencji, na przykład zakupionych wraz z zasobami wykorzystywanymi w lokalnym środowisku.

Dodatkowo rabat jest przyznawany w przypadku rezerwacji instancji. Dotyczy to subskrypcji proporcjonalnej do użycia oraz subskrypcji firmowej. Klient określa liczbę i rodzaje maszyn wirtualnych, z których zamierza korzystać w następnym okresie rozliczeniowym. Okres może obejmować rok lub dwa lata. W okresie dwuletnim rabat jest większy, ponieważ klient zobowiązuje się korzystać z usług przez dłuższy czas. W każdym momencie może zmienić warunki umowy, zwiększając lub zmniejszając liczbę maszyn. Po zwiększeniu przyznawany jest dodatkowy rabat, a po zmniejszeniu naliczane są kary.

Po wykupieniu subskrypcji można rezerwować zasoby i wdrażać swoje aplikacje. Zważywszy że oferta Microsoft Azure jest bardzo szeroka, decyzja, jakich zasobów używać i kiedy, nie jest prosta. Zanim zaczniesz się z nich korzystać, należy rozważyć kilka różnych strategii i modeli.

Do tej pory mówiliśmy o modelach IaaS, PaaS i SaaS. Przykładem modelu SaaS jest usługa Microsoft 365. Jest to oprogramowanie chmurowe dostępne w modelu subskrypcyjnym. Usługa ta jest dostępna nawet w centrach danych Azure (pierwotnym przeznaczeniem centrów było świadczenie tej usługi oraz zarządzanie tożsamością, dzisiaj noszącą nazwę usługi Azure Active Directory). Nie będziemy się jednak nią zajmować, ponieważ nie jest bezpośrednio związana z subskrypcjami Azure. Naszym celem jest poznanie różnic między modelami IaaS i PaaS.

IaaS jest pierwszym krokiem w procesie migracji zasobów do chmury, powszechnie akceptowanym przez specjalistów IT. W chmurze Azure maszynę wirtualną tworzy się bardzo łatwo i nie różni się ona zbyt wiele od wykorzystywanej w lokalnym środowisku. Klient nie ma dostępu do sprzętu i komponentów serwerów, dzięki czemu ich utrzymywanie jest prostsze i tańsze. Zarządzanie maszynami w chmurze Azure też nie wygląda inaczej niż w lokalnym

centrum danych, niezależnie od tego, jaka platforma wirtualizacyjna jest w nim wykorzystywana — Hyper-V, VMWare czy jeszcze inna. (W chmurze Microsoft Azure stosowana jest zmodyfikowana wersja Hyper-V, inna niż dla środowisk lokalnych).

Aby utworzyć maszynę, należy wybrać system operacyjny, wielkość dysku i kilka innych parametrów. Po utworzeniu należy się do niej podłączyć i zainstalować swoje oprogramowanie. Dostępem, bibliotekami, danymi i zainstalowanym oprogramowaniem zarządza użytkownik. Licencje otrzymuje w ramach subskrypcji lub może korzystać z własnych. Jeżeli utworzy maszynę z systemem operacyjnym Windows Server 2019 i bazą danych SQL Server 2019, będzie obciążany kosztami obu licencji.

Rezerwowanie zasobów w modelu PaaS jest jeszcze prostsze niż w IaaS. Łatwiej jest też nimi zarządzać. Klient nie ma jednak nad zasobami pełnej kontroli. Może modyfikować niektóre najważniejsze funkcjonalności, wartości określonych parametrów, włączać i wyłączać usługi. Niektóre rzeczy są jednak ustalone i nie ma możliwości ich zmiany. Ceny wszystkich licencji są z definicji uwzględnione w kosztach zasobów.

Przeanalizujmy prosty przypadek aplikacji WWW opartej na usłudze IIS (ang. Internet Information Services — internetowe usługi informacyjne) oraz bazie danych SQL Server.

W modelu IaaS trzeba utworzyć dwie maszyny wirtualne: jedną dla serwera WWW i drugą dla bazy danych. Aby uruchomić aplikację, trzeba na pierwszej maszynie zainstalować system operacyjny Windows Server 2019 oraz uruchomić usługę IIS. Na drugiej maszynie należy również zainstalować system operacyjny Windows Server 2019 oraz serwer bazy danych SQL Server 2019. W sumie trzeba zapłacić za zasoby, dwie licencje na system operacyjny Windows Server 2019 i jedną licencję na oprogramowanie SQL Server 2019, którego cena jest różna w zależności od wersji (Web, Standard lub Enterprise). Po zainstalowaniu oprogramowania i skonfigurowaniu usługi IIS trzeba zdefiniować zaporę i reguły bezpieczeństwa, dzięki którym będzie możliwy dostęp do aplikacji przez Internet. Oprócz tego należy skonfigurować komunikację między serwerem WWW a bazą danych, jak również zdefiniować odpowiednie reguły bezpieczeństwa. Jak widać, realizacja takiego prostego scenariusza w modelu IaaS wymaga mnóstwa pracy.

W modelu PaaS wystarczy jedynie zdefiniować plan usługi obejmującej serwer WWW oraz wykorzystywany przez niego serwer bazy danych SQL. Wszystkie licencje są już skonfigurowane i w tej części nie trzeba nic więcej robić. Cały proces jest znacznie prostszy i krótszy.

Z drugiej strony jednak model PaaS nie zawsze oferuje wszystko, co jest potrzebne do uruchomienia własnej aplikacji. Jeżeli na przykład potrzebna jest starsza wersja jakiejś platformy, wtedy PaaS nie sprawdzi się, ponieważ zdefiniowany jest w nim pewien zestaw platform i nie można instalować własnych. Jeżeli potrzebne są pewne funkcjonalności bazy danych, niedostępne w chmurze Azure, albo pojawia się problem z kompatybilnością oprogramowania, wówczas trzeba użyć maszyny wirtualnej z oprogramowaniem SQL Server.

Zazwyczaj model PaaS jest tańszy i prostszy w użyciu niż IaaS, ale ten drugi daje większą kontrolę i możliwość korzystania ze starszych wersji oprogramowania.

Oferta chmury Microsoft Azure nieustannie się powiększa i co kilka tygodni pojawiają się nowe usługi i funkcjonalności. W powyższym prostym przykładzie wymienionych jest tylko kilka z nich. IaaS daje wprawdzie użytkownikowi kontrolę nad tym, co znajduje się na maszynie wirtualnej, i oferuje szersze możliwości w porównaniu z pojedynczym zasobem, ale lista funkcjonalności w PaaS też nie jest zamknięta. Model ten umożliwia tworzenie usług aplikacyjnych, sieci CDN (ang. Content Delivery Network — sieć do dostarczania treści), baz danych, menedżerów ruchu, szyny usług, różnych funkcji, bazy CosmosDB i Redis, magazynów danych i wielu innych usług.

W modelu PaaS dostępnych jest ponad 50 różnego rodzaju usług przechowywania danych. Tak samo jest w przypadku serwisów WWW, mediów i przetwarzania danych. Wybór odpowiednich usług może okazać się bardzo korzystny finansowo i wydajnościowo. Należy jednak sprawdzać, czy dana usługa nie ma jakichś ograniczeń, do których usunięcia potrzebna byłaby inna usługa. Jeżeli się tego nie zrobi i nie rozważy wszystkich możliwych scenariuszy, wówczas skutek ograniczeń mogą się pojawić problemy z wydajnością aplikacji. Na szczęście w chmurze Azure klient nie jest związany z jednym rozwiązaniem i gdy stwierdzi, że popełnił błąd i wybrana przez niego usługa nie spełnia jego potrzeb, zawsze może ją zmodyfikować lub wybrać inną. Jest kilka kwestii, które należy rozważyć, decydując się na korzystanie z usług chmury Azure. Ceny niektórych zasobów są stałe, a innych uzależnione od stopnia użycia. Zasoby o stałej cenie niekiedy mają określone limity użycia i po ich osiągnięciu użytkownik jest obciążany dodatkowymi kosztami. W takim wypadku opłata stała zamienia się w opłatę zmienną. Od tej reguły są wyjątki w zależności od sposobu korzystania z zasobów.

Opłata za zasób o stałej cenie jest naliczana w chwili jego zarezerwowania. Cena obejmuje okres jednego miesiąca i jest dodawana do rachunku. Przykładami takich zasobów są usługi OMS (ang. Operations Management Suite — pakiet zarządzania operacjami) oraz Azure Active Directory w wyższych warstwach. Stały adres IP też jest zasobem o stałej cenie. Po zwolnieniu takiego zasobu do rachunku za bieżący okres rozliczeniowy jest doliczana kwota za dotychczasowe wykorzystanie.

Opłata za magazyn danych Azure jest uzależniona od jego stopnia wykorzystania. Użytkownik płaci za ilość przechowywanych danych, która każdego miesiąca może być inna. Ponadto na początku i końcu miesiąca danych może być mniej, a w środku okresu więcej. Dlatego wyliczane jest średnie wykorzystanie i na tej podstawie ustalana opłata.

Przykładem usługi z ograniczoną wydajnością jest transfer danych. Wysyłanie danych do chmury jest bezpłatne, podobnie jak ich pobieranie w ilości do 15 GB miesięcznie. Po przekroczeniu tego limitu naliczane są opłaty. Inne przykłady to rejestr kontenerów, w którym pierwsze 100 minut czasu procesora jest bezpłatnych, oraz funkcje Azure, które można za darmo wywoływać maksymalnie 1 milion razy.

Opłaty za korzystanie z zasobów obliczeniowych są naliczane co minutę. Na przykład opłaty za maszynę wirtualną lub usługę przestają być naliczane z chwilą zwolnienia tego zasobu. Zasada ta dotyczy również zaprzestania korzystania z zasobów w pewnych sytuacjach. Bazy danych SQL nie można zatrzymać i opłata jest naliczana co minutę. Przestaje być naliczana dopiero w momencie usunięcia bazy. Maszynę wirtualną lub usługę można zatrzymać i w ten sposób przestać płacić. Należy zwrócić uwagę na kilka niuansów związanych z opłatami za

maszyny wirtualne. Informacja o opłacie, widoczna podczas tworzenia maszyny wirtualnej i wykorzystywana w kalkulatorze, dotyczy tylko jej czasu pracy. Ale maszyna wykorzystuje magazyn danych, za który są naliczane opłaty niezależnie od tego, czy maszyna działa, czy nie. Koszty powiększają też niektóre komponenty sieciowe, na przykład publiczny adres IP, za który pobierana jest osobna opłata.

Dlatego bardzo ważne jest kontrolowanie wykorzystania zasobów i znajomość dopuszczalnych limitów. Za niektóre zasoby mogą być naliczane dodatkowe opłaty, jeżeli nie korzysta się z nich umiejętnie, a nawet gdy nie korzysta się wcale. Na tym polega różnica w porównaniu z tradycyjnym środowiskiem IT, w którym za zasoby płaci się z góry i nie ma znaczenia, czy maszyna wirtualna jest wykorzystywana, czy nie, o ile tylko nie zostaną wyczerpane zasoby sprzętowe. W Azure płaci się za wszystkie rezerwowane (lub wykorzystywane) zasoby, dlatego trzeba je kontrolować i porównywać z aktualnymi potrzebami. W przeciwnym wypadku rachunki będą coraz wyższe i chmura może się okazać bardzo drogim rozwiązaniem. Oszczędności finansowe mogą być znaczne, ale jeżeli nie zachowa się ostrożności, efekt będzie odwrotny do zamierzonego. Miałem do czynienia z wieloma firmami, które tworzyły środowiska programistyczne i testowe bez żadnej kontroli. Wiele zasobów było rezerwowanych nie wiadomo po co i przez kogo, nie mówiąc o sprawdzaniu, czy faktycznie były wykorzystywane. W środowiskach produkcyjnych to się raczej nie zdarza, ale w innych sytuacjach owszem. W 2014 r. Microsoft ogłosił nowe wcielenie chmury Azure ze zmienionym portalem i z modelem ARM. Pisałem już, jak modele ARM i RBAC zmieniły sposób administrowania zasobami i jak bardzo ułatwiły korzystanie z chmury.

Nowością w modelu ARM są szablony, czyli pliki w formacie JSON zawierające informacje o wszystkich zasobach umieszczonych w grupie zasobów. Szablony wykorzystuje się do rezerwowania, modyfikowania i zwalniania zasobów. Każda grupa zasobów w portalu ma mechanizm umożliwiający tworzenie szablonów, pobieranie ich na lokalny dysk i rozszerzanie o kolejne zasoby. Dzięki temu zasoby można szybko i łatwo powielać.

Umieszczanie zasobów w jednej aplikacji jest często stosowaną praktyką, bardzo przydaną w przypadku, gdy środowisko jest skomplikowane i jego wdrożenie zajmuje dużo czasu. Załóżmy, że mamy farmę serwerów SharePoint, maszynę z systemem Windows Server pełniącą rolę kontrolera domeny i dwie dodatkowe maszyny z bazą danych SQL Server. Aby uruchomić takie środowisko, trzeba utworzyć wirtualną sieć i pięć maszyn, a następnie połączyć wszystko ze sobą. Ręczne wykonanie tych operacji zajmuje jakiś czas. Natomiast za pomocą szablonów ARM można to zrobić w kilka sekund.

Wdrażanie infrastruktury przy użyciu szablonów jest jedną z opcji modelu IaC. Podobny efekt można osiągnąć za pomocą skryptu PowerShell i konsoli Azure CLI. W powyższym modelu można szybko i niezawodnie kreować infrastruktury niezbędne do uruchamiania aplikacji. Szablony zwalniają użytkownika z ręcznego wykonywania operacji, automatyzują procesy i zapobiegają pomyłkom.

Inną zaletą szablonów ARM jest możliwość umieszczania ich w projektach aplikacji i zapisywania w repozytorium. Dzięki temu można kontrolować wersje środowisk. Poszczególne wersje aplikacji mogą wymagać wprowadzania zmian w środowisku. Za pomocą szablonów i repozytoriów kodu można śledzić wprowadzane zmiany. Daje to

pewność, że utworzone środowisko jest odpowiednie dla uruchamianej aplikacji. Szablony ARM zapewniają szybki, niezawodny i spójny sposób rezerwowania zasobów Azure. Dzięki nim można kontrolować wersje środowisk i automatyzować procesy wdrażania oprogramowania. Szablony okazują się szczególnie przydatne w implementacji metodyki DevOps w procesie dostarczania oprogramowania. W połączeniu z modelem „konfiguracja jako kod” można tworzyć i replikować środowiska zawierające niezbędne zasoby skonfigurowane tak, aby wszystko działało poprawnie.

Oto przykładowy szablon ARM:

```
{
  "$schema":
    "https://schema.management.azure.com/schemas/2015-01-01/
    □deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
  },
  "variables": {
  },
  "resources": [
  ],
  "outputs": {
  }
}
```

Szablon zawiera sekcje parametrów (parameters), zmiennych (variables), opisów zasobów (resources) i wyników (outputs). Informacje te definiują zasoby, które mają być zarezerwowane z określonymi parametrami. Zmienne umożliwiają modyfikowanie wartości parametrów, a opcjonalne wyniki służą do sprawdzania poprawności przebiegu procesu.

Podsumowując w tym pierwszym wprowadzającym wykładzie chciałem przedstawić podstawowe pojęcia, terminy oraz możliwości wszystkich rodzajów chmur ze szczególnym naciskiem na rozwiązania Azure. Większość terminów takich jak IASS, PAAS etc mają zastosowanie do innych rozwiązań chmurowych.

Dziękuję za przeczytanie