PARP Grupa PFR / Centrum Rozwoju MŚP

Co to są usługi chmurowe i jak z nich korzystać?

Kamil Mrzygłód

31 sierpnia 2022 r.

Plan prezentacji:

1. Definicja usług chmurowych.
2. Chmura vs rozwiązania on-premises.
3. Chmura publiczna / hybrydowa / prywatna.
4. IaaS / PaaS / SaaS oraz pochodne.
5. Koszty chmury.
6. Gwarancje dostawców chmury.
7. Optymalizacja kosztów.
8. Chmura w kontekście regulacji.
9. Bezpieczeństwo rozwiązań chmurowych.
10. Chmura a rynek pracy.

Definicja usług chmurowych

Powrót do spisu treści

Elementy usług chmurowych

- Infrastruktura (fizyczna oraz zwirtualizowana)
- Usługi towarzyszące
- Interfejs usługi (zarówno graficzny [UI], jak i programistyczny [API])
- Resource Provider
- SDK
- Kod oraz konfiguracja usługi

Definicja usług chmurowych

Usługa chmurowa to gotowy produkt (SaaS) bądź półprodukt (IaaS / PaaS), hostowany oraz udostępniany w ramach współdzielonej infrastruktury fizycznej wybranego dostawcy chmurowego. Każda usługa chmurowa rozliczana jest w oparciu o z góry ustalony model płatniczy na zasadach zawartych w umowie pomiędzy usługodawcą a usługobiorcą.

Definicja usług chmurowych

Usługi chmurowe od tradycyjnych form hostowania infrastruktury oraz aplikacji wyróżnia:

- Skala dostępnej infrastruktury chmurowej
- Łatwość replikacji geograficznej
- Sposoby rozliczania (użycie zgodne z użyciem [PAUG], płatność minutowa, sekundowa, per wirtualne metryki gwarantowanej przepustowości usługi)
- Znacznie większy poziom abstrakcji pomiędzy infrastrukturą fizyczną a zwirtualizowaną
- Wysoka dynamika i zmienność środowiska

Powrót do spisu treści

Chmura vs rozwiązania on-premises

On-premises

- Lokalna infrastruktura fizyczna, nad którą mamy pełną kontrolę
- Standardowy i dobrze znany model hostowania aplikacji
- Wymaga wydzielenia fizycznego miejsca na składniki infrastruktury oraz:
  - Zapewnienie redundancji systemów zasilania, chłodzenia, bezpieczeństwa
  - Zagwarantowania odpowiednich polityk oraz regulacji determinujących zasady dostępu do fizycznej infrastuktury
  - Ubezpieczenia infrastruktury, jak i danych tam składowanych
  - Spełnienia wymogów regulacyjnych w przypadku procesowania danych wymagających odpowiednich certyfikatów
  - Regularnej konserwacji
  - Zatrudnienia zespołu odpowiedzialnego za utrzymanie infrastruktury

Chmura vs rozwiązania on-premises

Oryginalny kierunek migracji

- Początkowo wiele firm kierowało się ze środowisk on-premises do chmury bez planu powrotu
- Obecnie coraz częściej widać potrzebę wykorzystania środowisk hybrydowych, które pozwalają na koegzystowanie obu modeli hostowania aplikacji
- Zmiana trendu związana jest zarówno z trudnościami natury prawnej (przetwarzanie danych w miejscach, które są poza granicami kraju, z którego pochodzą), logistycznej (infrastruktura chmurowa poza granicami naszego kraju przy jednoczesnej potrzebie komunikacji ze środowiskami on-premises), wydajnościowej (aplikacje projektowane na środowiska on-premises nie są dostosowane do działania w środowiskach chmurowych), a także nieosiągnięciem spodziewanej wartości współczynnika Value vs Effort

Chmura vs rozwiązania on-premises

Obecny kierunek migracji

- Nacisk na środowiska hybrydowe w oparciu o zdefiniowany katalog usług wraz z ich bazowymi założeniami
- Wykorzystanie środowisk chmurowych w miejscach, gdzie możliwe jest dynamicze skalowanie *naszych* aplikacji
- Cloud bursting – infrastruktura chmurowa jest traktowana jako “przedłużenie” naszej lokalnej infrastruktury, które umożliwia bardzo szybkie skalowanie horyzontalne bez konieczności posiadania zapasu infrastruktury fizycznej
- Przenoszenie do chmury elementów, co do których brakuje nam know-how i nie planujemy poszerzenia naszych kompetencji w tych obszarach (ML, AI, Kubernetes, architektury mikroserwisowe, load balancing, bezpieczeństwo)

Chmura vs rozwiązania on-premises

Różnice w kosztach

- Środowiska on-premises rozliczane są w całkowicie innym modelu niż usługi chmurowe
  - W przypadku naszych własnych środowisk fizycznych, jesteśmy odpowiedzialni za zakup sprzętu, jego konfigurację, utrzymanie
  - Wszystkie te elementy powinny być brane przed nas pod uwagę w przypadku porównywania kosztów z chmurą
  - Brak określenia tzw. Total Cost of Ownership (TCO) jest częstym błędem przy określaniu finansowych aspektów migracji do chmury
- Chmura obliczeniowa jest bazowo droższa
  - W chmurze trudniej jest ukryć poszczególne składowe kosztów, ale nie widzimy jak koszt jest rozkładany na metryki, którymi posługujemy się w środowiskach on-premises
  - Powoduje to problem ze wskazaniem elementów, które można optymalizować w celu ograniczenia finalnego rachunku za usługi chmurowe
  - Usługi chmurowe pozwalają często na tzw. rezerwacje, które potrafią zmniejszych koszt usługi nawet o 40%
  - Firmy jednak często obawiają się rezerwacji z powodu tzw. wymogu “commitmentu”, który trwa od 12 do 36 miesięcy i niejako predefiniuje ile czasu będziemy z tej usługi korzystać

Powrót do spisu treści

Chmura publiczna/ prywatna/ hybrydowa

Chmura publiczna

- Bazowy model chmury obliczeniowej oparty o publicznie dostępną infrastrukturę dostawcy
- Uproszczona konfiguracja skupiająca się głównie na wykorzystaniu zarządzalnych komponentów i usług bez ich integracji z własną siecią oraz infrastrukturą on-premises
- Problematyczna w przypadku konieczności komunikacji z odizolowanymi komponentami, szczególnie w przypadku usług w modelu SaaS
- Możliwa do wykorzystania przez każdego klienta
- Oparta o założenie, że klienci mogą współdzielić tę samą infrastrukturę fizyczną

Należy pamiętać, że w zależności od dostawcy definicja chmury publicznej/ prywatnej może się różnić, a oferta chmury publicznej może zawierać element chmury prywatnej.

Chmura publiczna/ prywatna/ hybrydowa

Chmura prywatna

- Dedykowana infrastruktura przeznaczona dla danego klienta
- Często oferowana przez dostawców jako element oferty chmury publicznej
- Gwarantuje izolację od innych klientów, także na poziomie infrastruktury fizycznej
- Przydatna wszędzie tam, gdzie wymogi regulacyjne nie pozwalają nam na współdzielenie fizycznych komponentów, na których bazuje nasza infrastruktura
- Z racji bycia dedykowanym rozwiązaniem, na ogół jest droższa i wymaga większych nakładów po naszej stronie (konfiguracja oraz utrzymanie)

Chmura publiczna/ prywatna/ hybrydowa

Chmura hybrydowa

- Rozwiązanie łączące elementy chmury publicznej oraz prywatnej
- Coraz większa popularność wynikająca z lepszego odwzorowania realiów biznesowych
- Dość skomplikowany model wynikający z konieczności zarówno integracji elementów chmury publicznej oraz prywatnej, a także wymogu odpowiedniego zaprojektowania naszego środowiska, jak i zapewnienia ujednoliconego sposobu zarządzania
- Często wykorzystuje dedykowane połączenia do infrastruktury dostawcy chmurowego w celu zagwarantowania wymaganego poziomu bezpieczeństwa oraz izolacji
- Chmura hybrydowa oznacza także połączenie chmury prywatnej oraz systemów on-premises

Chmura publiczna/ prywatna/ hybrydowa

Zastosowania chmury publicznej

- Rozwiązania dedykowane dla użytkowników końcowych niebędących naszymi pracownikami bądź partnerami
- Systemy niewymagające dedykowanej infrastruktury fizycznej
- Aplikacje, które dopuszczają ich zabezpieczenie za pomocą komponentów chmury publicznej (firewalle/ sieci wirtualne)

Zastosowania chmury prywatnej

- Aplikacje intranetowe
- Systemy przetwarzające dane, których charakterystyka wymaga spełnienia określonych wymagań (np. dane personalne)
- Procesy o rygorystycznych wymaganiach wydajnościowych, które nie gwarantują poprawnego działania w przypadku działania w ramach współdzielonej infrastruktury fizycznej

Zastosowania chmury hybrydowej

- Aplikacje oraz systemy, które są w stanie funkcjonować w oparciu o komponenty dostępne zarówno w ramach infrastruktury publicznej, jak i prywatnej
- Modernizacja aplikacji i skalowanie lokalnej infrastruktury

Powrót do spisu treści

IaaS/ PaaS/ SaaS oraz pochodne

W ramach chmury obliczeniowej, dostępne usługi są oferowane w różnych modelach:

- IaaS – Infrastructure-as-a-Service
- PaaS – Platform-as-a-Service
- SaaS – Software-as-a-Service

W ramach rozwoju usług chmurowych, ukute zostały kolejne modele:

- FaaS – Function-as-a-Service
- Serverless
- DBaaS – Database-as-a-Service
- CaaS – Containers-as-a-Service

Wszystkie pochodne modele bazują na 3 bazowych modelach.

IaaS/ PaaS/ SaaS oraz pochodne

Infrastructure-as-a-Service

- Model usług chmurowych najbardziej zbliżony do tradycyjnej infrastruktury on-premises
- Skupia się na dostarczeniu klientowi usług pozwalających na samodzielne zbudowanie zwirtualizowanej infrastruktury takich jak maszyny wirtualne, sieci wirtualne, load balancery, adresy IP, backupy
- IaaS wymaga dość znacznych nakładów finansowych z racji swojej charakterystyki – wymagana jest znajomość budowania infrastruktury aplikacji, segmentacji sieci, gwarantowania dostępności w oparciu o niskopoziomowe komponenty infrastrukturalne
- IaaS jest często pierwszym krokiem w ramach migracji do chmury (lift & shift)
- Obecnie widoczny jest trend, w ramach którego firmy odchodzą powoli od modelu IaaS na korzyść modeli PaaS/ SaaS
- Jednocześnie IaaS pozostaje jedynym modelem chmurowym, który pozwala na dostęp do ustawień systemu operacyjnego maszyn wirtualnych

IaaS/ PaaS/ SaaS oraz pochodne

Platform-as-a-Service

- Ewolucja modelu IaaS
- Większy poziom abstrakcji w stosunku do IaaS na korzyść łatwiejszego zarządzania
- Obecnie cel wielu migracji do chmury obliczeniowej
- Migracje do PaaS nie mogą być wykonane w prostym modelu lift & shift – wymagana jest modernizacja architektury oraz kodu aplikacji
- Pierwszy model, w ramach którego mówimy o architekturach cloud native
- Na ogół model PaaS reprezentuje najliczniejszą ofertę usług chmurowych – w ramach niego mamy dostęp do zarządzalnych baz danych, komponentów do hostowania aplikacji webowych, uruchamiania skonteneryzowanych aplikacji w chmurze czy systemów kolejkowych
- PaaS może być traktowany jako rozwiązanie pośrednie pomiędzy IaaS a SaaS

IaaS/ PaaS/ SaaS oraz pochodne

Software-as-a-Service

- Model dostępny nie tylko w ramach chmury obliczeniowej
- Opiera się o dostarczenie gotowego produktu do klienta końcowego
- Odpowiedzialnością klienta jest takie skonfigurowanie dostarczonej usługi, aby realizowała założone wymagania biznesowe
- SaaS jest modelem, który traktujemy jak tzw. black box. Nie mamy dostępu do kodu, nie jesteśmy odpowiedzialni za architekturę takich usług
- W przypadku chmury SaaS można traktować jako usługi, które poza bazową konfiguracją nie zezwalają nam na głębszą ingerencję w infrastrukturę usługi (często spotykany model w ramach usług od ML/ AI/ security)
- Pozwala na szybką integrację oraz prototypowanie, w przypadku bardziej skomplikowanych systemów SaaS może okazać się niewystarczający z powodu ograniczeń konfiguracyjnych oraz zależności od zewnętrznego dostawcy

IaaS/ PaaS/ SaaS oraz pochodne

Inne modele

- Chmura oferuje usługi także w innych modelach niż IaaS/ PaaS/ SaaS, jednak na ogół jest to tylko i wyłącznie marketingowy chwyt, bazowo są to usługi działające w ramach wymienionych wyżej modeli
- Niektóre usługi oferowane są w modelu serverless, który charakteryzuje się nieco inną specyfiką działania
    - Serverless jest dostępny zarówno w ramach usług FaaS pozwalających na uruchamianie fragmentów kodu, jak i baz danych gdzie baza jest aktywowana tylko w momencie, gdy jest potrzebna. Głównym wyróżnikiem takich usług jest płatność za czas, kiedy usługa była aktywna – w przypadku braku wykorzystania, nie jesteśmy obciążani opłatą.
- Zdarza się, że dostawcy chmurowi oferują gotowe zewnętrzne produkty (jak np. Kubernetes) jako swój produkt (Azure Kubernetes Service/ Google Kubernetes Engine/ AWS Elastic Kubernetes Service)

Powrót do spisu treści

Koszty chmury

Chmura vs on-premises

- Bazowo chmura na ogół jest droższa od innych form hostowania aplikacji
- Należy dokładnie policzyć TCO i upewnić się, że porównując oba środowiska bierzemy pod uwagę wszystkie składowe
- Wykorzystanie chmury daje nieco inne możliwości niż on-premises (i vice versa), należy więc dokładnie określić jaką wartość biznesową otrzymujemy używając danego środowiska

Koszty chmury

Kalkulacja kosztów chmury

- Dostawcy chmurowi oferują gotowe kalkulatory, które upraszczają wykonanie wstępnej estymaty kosztów
- Należy pamiętać, że kalkulacja kosztów wymaga znajomości danych usług, architektury systemu oraz jego charakterystyk
- Nieznajomość technikaliów własnych systemów jest często powodem niedoszacowania kosztów architektury opartej o chmurę
- Dostawcy chmurowi często oferują zniżki oraz rezerwacje na usługi, które zmniejszają ogólny koszt
- O ile zniżki to jest kwestia indywidualnych negocjacji oraz przyjętego modelu rozliczeń, rezerwacje są dostępne dla wszystkich w tej samej formie
- Jeśli nie mamy doświadczenia, kalkulację kosztów należy zlecić doświadczonej osobie, która rozumie dogłębnie sposób rozliczania danego dostawcy chmurowego

Koszty chmury

FinOps

- FinOps jest podejściem, które zakłada zbudowanie know how oraz procesu związanego z kalkulacją kosztów chmury w sposób ciągły
- Bazuje na zrozumieniu poszczególnych składowych kosztów chmury, a także wykorzystaniu narzędzi, które pozwalają nie tylko raportować koszt, ale także estymować go przed wprowadzeniem zmian
- Może być używany w tandemie z podejściem CICD, w ramach którego zmiany wprowadzane do aplikacji oraz systemów są na bieżąco weryfikowane i prezentowane w formie artefaktów

Powrót do spisu treści

Gwarancje dostawców chmury

SLA

- Każdy z dostawców chmury oferuje indywidualne gwarancje związane z zagwarantowanie dostępności komponentów chmurowych
- W przypadku chmury publicznej, głównym parametrem jest SLA, które określa spodziewany poziom działania usługi bez awarii
- Należy pamiętać, że dedykowane rozwiązania chmurowe charakteryzują się całkowicie innym poziomem gwarancji dostępności niż chmura publiczna, co wynika z całkowicie innych potrzeb i dostępnych narzędzi

Gwarancje dostawców chmury

Przekroczenie SLA

- W przypadku przekroczenia SLA przez naszego dostawcę, przysługuje nam rekompensata zależna od poziomu niedostępności usługi chmurowej
- Należy pamiętać, że w przypadku usług chmury publicznej, rekompensata jest oparta o nasze wydatki na daną usługę, a nie wysokość strat, które ponieśliśmy w wyniku awarii
- Nasz dostawca chmurowy nie oferuje rekompensaty automatycznie – poprzez zbieranie odpowiednich metryk musimy samodzielnie przygotować specjalny raport, który potwierdzi, że byliśmy dotknięci awarią
- Środki pieniężne w ramach rekompensaty są na ogół transferowane na kolejny okres rozliczeniowy

Gwarancje dostawców chmury

RTO/ RPO

- Usługi chmury publicznej rzadko kiedy są oferowane wraz ze zdefiniowanymi parametrami RTO/ RPO
- Utrudnia to projektowanie architektury chmurowej na tych samych zasadach co systemy on-premises, gdzie na ogół RTO/ RPO są zawarte w ramach wymagań biznesowych
- Niektóre usługi chmurowe (jak np. bazy danych) mają oficjalnie zdefiniowane RTO/ RPO, a także oferują specjalne tiery (np. business critical) dające wyższe gwarancje dostępności
- Poprzez dopasowanie do specyfiki naszej firmy, chmura prywatna może nam zagwarantować odpowiedni poziom RTO/ RPO

Powrót do spisu treści

Optymalizacja kosztów

Metody optymalizacji

- Rezerwacje
  - Pozwalają na zmniejszenie kosztów poszczególnych usług poprzez tzw. commitment – wykupienie usługi z góry na określony okres czasu (najczęściej 12 lub 36 miesięcy)
  - Wysokość zniżki uzależniona jest od wykupionego okresu (rośnie wraz z wydłużeniem okresu)
  - Pozwalają obniżyć koszty usługi nawet o połowę
  - Najczęściej dostępne dla maszyn wirtualnych oraz magazynów danych
- Przenoszenie licencji
  - W ramach środowisk on-premises często posiadamy licencje (np. Windows Server), które generują określony koszt
  - W momencie wykupienia usługi w chmurze, jej cena zawiera w sobie bardzo często koszt tej samej licencji, którą wcześniej wykupiliśmy na potrzeby naszego lokalnego środowiska
  - Niektórzy dostawcy chmurowi pozwalają na przeniesienie wykupionej wcześniej licencji do środowiska chmurowego
  - W połączeniu z rezerwacją uzyskujemy często zniżkę na poziomie 70% - 80% od bazowego kosztu usługi

Optymalizacja kosztów

Metody optymalizacji

- Konta dev/ test
  - Na potrzeby testów oraz codziennego development możemy często skorzystać z wersji usług, które oferują niższe SLA w zamian za niższy koszt
  - Jest to przydatna opcja dla kreowania nieprodukcyjnych środowisk, które posiadają niższe wymagania pod kątem dostępności oraz stabilności usług chmurowych
- Low-priority/ spot instances
  - Niektóre usługi oferują specjalne wersje low-priority/ spot, które charakteryzują się bardzo niskim bądź brakiem SLA
  - Ich dodatkową cechą jest fakt „wywłaszczania” – w momencie ograniczonej dostępności mocy obliczeniowej w data centre naszego dostawcy, klienci korzystający ze standardowych wersji usług mogą automatycznie wywłaszczać innych klientów korzystających z niskopriorytetowych wersji
  - Tego typu wersje usług są szczególnie przydatne w ramach krótkożyjących komponentow jak np. agenci dla CICD, nieprodukcyjne klastry Kubernetes, bezstanowe usługi

Optymalizacja kosztów

Metody optymalizacji

- Housekeeping
  - Dużym problemem w ramach usług chmurowych jest brak housekeepingu, czyli kontroli istniejących instancji usług chmurowych pod kątem ich użycia
  - W trakcie developmentu powstaje często wiele artefaktów infrastrukturalnych, które potem nie są usuwane generując koszty
  - Stała kontrola zasobów pozwala na wcześniejsze wykrycie niepotrzebnych elementów i ich usunięcie
- Serverless/ pay-as-you-go
  - Metodą optymalizacji kosztów jest także wykorzystanie usług w modelu serverless/ pay-as-you-go, co pozwala na ograniczenie kosztów w przypadku aplikacji, które są używane sporadycznie
  - Metoda ta nie sprawdzi się jednak w przypadku aplikacji o standardowej charakterystyce użycia a może nawet wygenerować większe koszty
  - Minusem niektórych usług w modelu serverless są ograniczone możliwości jeśli chodzi o np. integrację z sieciami wirtualnymi

Powrót do spisu treści

Chmura w kontekście regulacji

Informacje ogólne

- Chmura, jak każda inna usługa czy narzędzie, musi być zweryfikowana pod kątem regulacji, które narzucają na nasze systemy odpowiednie wymagania
- Każdy z dostawców chmurowych publikuje zestaw dokumentów, które określają zasady korzystania z ich usług, gwarancje czy informacje, w jaki sposób realizują wymogi poszczególnych regulacji:
  - Privacy statement
  - Data protection
  - Service Level Agreement

Chmura w kontekście regulacji

Regulacje a dostawca

- W zależności od wymogów regulacyjnych, wybór naszego dostawcy może być ograniczony
- Większość wiodących dostawców chmury spełnia popularne wymogi oraz standardy
- W przypadku wymogu spełnienia przez infrastrukturę określonych reguł (EU-U.S Privacy Shield, EU Model Clauses, HIPAA/HITECH, HITRUST) musimy zweryfikować, czy nasz dostawca jest w stanie zagwarantować odpowiedni poziom świadczonych usług

Chmura w kontekście regulacji

GDPR (General Data Protection Regulation)

- W przypadku konieczności spełnienia wymogów związanych z GDPR, wielu dostawców dostarcza specjalne narzędzia, które pozwalają na wykrycie oraz sklasyfikowanie danych, które są objęte regulacjami GDPR
- Jednocześnie część pracy musi być wykonana po naszej stronie (przykładowo – wymuszenie centralnie wykorzystania tylko określonych regionów chmurowych)
- Niektórzy dostawcy dostarczają dodatkowe narzędzia, które pozwalają skanować infrastrukturę on-premises pod kątem wrażliwych danych, co pozwala na szybkie skatalogowanie posiadanych rekordów i podjęcie odpowiednich kroków pod kątem ich zabezpieczenia

Bezpieczeństwo rozwiązań chmurowych

Shared Model Responsibility

- Chmura zobowiązuje nas to wzięcia części odpowiedzialności za bezpieczeństwo naszej infrastruktury oraz aplikacji
- W zależności od wykorzystanego modelu usług (IaaS/ PaaS/ SaaS) poziom odpowiedzialności będzie się różnić:
  - IaaS nakłada na nas największą odpowiedzialność z racji dostępu do systemu operacyjnego maszyn wirtualnych, co wymusza na nas konieczność aktualizacji samego systemu, jak i zainstalowanych aplikacji
  - SaaS jest modelem, w ramach którego nasza odpowiedzialność skupia się głównie na poprawnej implementacji rozwiązania oraz nadania odpowiednich poziomów uprawnień
- Niezależnie od modelu usług, odpowiedzialność za infrastrukturę fizyczną spoczywa na dostawcy
- Należy pamiętać, że w przypadku korzystania z dedykowanego rozwiązania chmurowego, poziom odpowiedzialności za całość rozwiązania może spoczywać całkowicie na dostawcy, co odróżnia ten model od chmury publicznej
- Chmura publiczna pod kątem bezpieczeństwa jest wystarczająca dla większości rozwiązań z racji skomplikowania całości zagadnienia i braku odpowiedniego know-how w wielu firmach

Powrót do spisu treści

Bezpieczeństwo rozwiązań chmurowych

Gwarancje bezpieczeństwa

- Chmura publiczna zapewnia odpowiedni poziom bezpieczeństwa (zdefiniowany w ramach oficjalnych dokumentów naszego dostawcy) oraz implementację odpowiednich procedur (np. pod kątem usuwania danych), należy jednak pamiętać, że nasz dostawca nie jest na samym końcu bezpośrednio odpowiedzialny za bezpieczeństwo naszych rozwiązań
- Dostawcy na ogół świadczą usługi na zasadzie “best effort” co oznacza, że ciężko jest im udowodnić świadome działanie, na niekorzyść klienta, jeśli z ich winy pojawi się dziura bezpieczeństwa w systemie
- Jednocześnie głównym wektorem ataku na chmurę są sami klienci – głównym problemem na ogół jest niewłaściwa konfiguracja, brak odpowiedniej segmentacji sieci czy nieprawidłowe skonfigurowanie zabezpieczeń

Powrót do spisu treści

Chmura a rynek pracy

Specjaliści chmurowi

- Obecnie na rynku jest coraz więcej specjalistów, którzy mają doświadczenie z chmurą
- Z drugiej strony znalezienie bardzo doświadczonego pracownika w ramach danej dziedziny (infrastruktura/ bazy danych /development) może być problematyczne z racji dużej konkurencji oraz obecności zachodnich firm na rynku, które dodatkowo zmniejszają pulę osób dostępnych na rynku
- Dodatkowym problemem jest zróżnicowanie dostawców chmury – specjalista od jednego dostawcy niekoniecznie ma kompetencje do pracy z innym dostawcą

Chmura a rynek pracy

Szkolenia

- Z racji trudności w dostępie do wyszkolonych specjalistów związanych z chmurą, pewnym rozwiązaniem może być rozbudowywanie kompetencji naszych pracowników poprzez szkolenia
- Na rynku dostępne jest wiele szkoleń dostosowanych do poziomu uczestników oraz faktycznych zagadnień do poruszenia
- Możemy rozważyć także dedykowane szkolenia nakierunkowane na rozwiązanie opisanego problemu

Kontakt
tel.: +48 505 081 294
e-mail: kamil@thecloudtheory.pl
www.thecloudtheory.com