Poznajemy chmurę

Opowieść i mapa książki.

- Chmura: cudzy komputer, za który płacimy za minutę

Chmura: cudzy komputer, za który płacimy za minutę

Poziom: podstawy **Dotyczy: Amazon S3, Amazon EC2, Microsoft Azure**

Czas: ~10 min

Ta strona otwiera książkę o chmurze: skąd wziął się pomysł na wynajmowanie cudzych komputerów za minuty pracy, co w tym modelu należy do dostawcy, a co do nas, i co czeka na kolejnych stronach.

Skróty użyte na tej stronie (3)

Skrót	Co znaczy
EC2	Elastic Compute Cloud: usługa AWS wynajmująca gotowe maszyny wirtualne na godziny
PDC	Primary Domain Controller: rola FSMO (PDC Emulator) pełniąca funkcje historycznie zarezerwowane dla podstawowego kontrolera domeny, dziś głównie synchronizację czasu i zmiany haseł
S3	Simple Storage Service: magazyn plików w chmurze AWS

Skąd się wzięło

Pomysł na chmurę jest starszy niż internet. W latach sześćdziesiątych pojedynczy mainframe kosztował więcej niż budynek, w którym stał, więc uczelnie i firmy dzieliły jego czas między wielu użytkowników naraz, w systemie zwanym time sharing. Każdy użytkownik logował się z osobnego terminala, dostawał swój wycinek czasu procesora, i miał wrażenie, że komputer pracuje wyłącznie dla niego, choć w tle obsługiwał dziesiątki innych osób. To właśnie ten model, płać za wykorzystany czas zamiast za cały sprzęt, wrócił kilkadziesiąt lat później pod nazwą chmury.

Nowoczesną chmurę publiczną otworzył Amazon, firma, która zbudowała ogromną infrastrukturę na własne potrzeby sklepu internetowego i zauważyła, że większość czasu stoi ona bezczynnie poza sezonem świątecznym. 14 marca 2006 roku Amazon uruchomił Simple Storage Service, w skrócie S3: usługę do przechowywania dowolnych plików w internecie, płatną od gigabajta i liczby zapytań, bez własnego serwera plików. Pięć miesięcy później, 25 sierpnia 2006 roku, dołączył Elastic Compute Cloud, w skrócie EC2, pozwalający wynająć cały wirtualny serwer na minuty lub godziny, zamiast kupować fizyczną maszynę na lata.

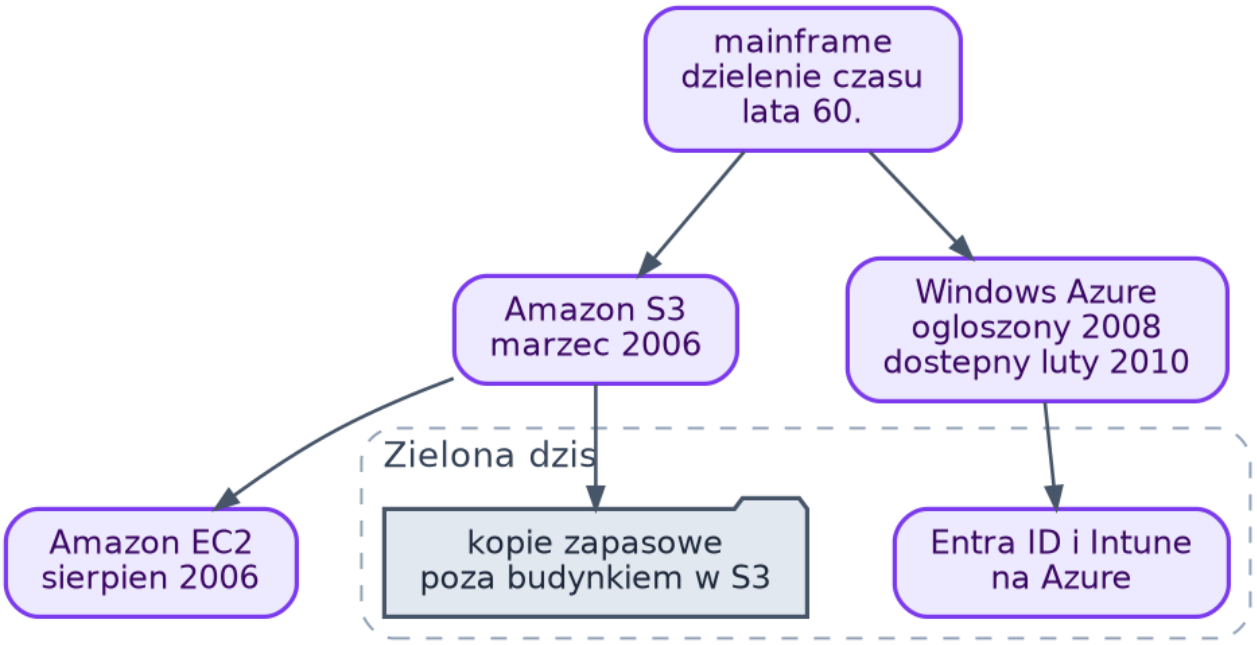
> **Pojęcie: IaaS.** Infrastructure as a Service, model chmury, w którym dostawca daje nam gołą maszynę wirtualną, dysk i sieć, a systemem operacyjnym i wszystkim ponad nim zarządzamy sami, tak jak z EC2.

Microsoft dołączył do wyścigu z pewnym opóźnieniem: usługę Windows Azure zapowiedziano na konferencji PDC w październiku 2008 roku, a publicznie dostępna, płatna wersja ruszyła 1 lutego 2010 roku. W 2014 roku usługę przemianowano na Microsoft Azure, żeby podkreślić, że oferuje więcej niż tylko maszyny z Windowsem. Od tego czasu obaj giganci, razem z Google Cloud, rywalizują na tym samym rynku, oferując coraz więcej gotowych usług ponad samą infrastrukturą.

Razem z rosnącą liczbą usług powstał model współodpowiedzialności: dostawca chmury odpowiada za bezpieczeństwo samej infrastruktury, serwerowni i sieci szkieletowej, a klient odpowiada za to, co na niej uruchamia, od systemu operacyjnego po hasła i uprawnienia. Głośne wycieki danych z niewłaściwie skonfigurowanych kubełków S3 przypominają, że przejście do chmury nie oddaje tej odpowiedzialności dostawcy.

Jak to działa w jednym obrazku

> **Pojęcie: model współodpowiedzialności.** Podział obowiązków między dostawcę chmury a klienta: dostawca pilnuje bezpieczeństwa sprzętu, sieci i wirtualizacji, a klient pilnuje bezpieczeństwa wszystkiego, co sam na tej infrastrukturze skonfigurował i uruchomił.



Od mainframe'a przez S3 i EC2 do Azure: rodowód chmury publicznej i miejsce usług w Zielonej (kliknięcie otwiera pełny rozmiar)

Dlaczego Zielona

> **Z ŻYCIA WZIĘTE**
>
> Pan Zbigniew z księgowości przynosi Tomkowi wydruk faktury od Amazona i pyta, dlaczego w zeszłym miesiącu opłata skoczyła trzykrotnie. Tomek sprawdza panel kosztów i znajduje odpowiedź: ktoś testował pobieranie całego archiwum kopii zapasowych z S3 na laptopa w biurze, zamiast na serwer w tej samej chmurze. Ruch wychodzący z S3 do internetu, w odróżnieniu od ruchu przychodzącego, jest płatny za każdy gigabajt, i to on podbił rachunek.

Od tamtej rozmowy Zielona trzyma w S3 wyłącznie to, co ma tam zostać: kopie zapasowe poza budynkiem, opisane na stronie Backup bazy do S3: agent backint i jego ograniczenia, pobierane z powrotem tylko w razie realnej awarii, nigdy rutynowo. Do codziennej pracy zespół korzysta z Azure, gdzie działają Entra ID i Intune: pierwsze zarządza kontami i logowaniem, drugie konfiguracją i zgodnością firmowych i prywatnych urządzeń, opisanych bliżej na stronie Urządzenia służbowe i prywatne: BYOD, COPE, COBO.

Taki podział, S3 jako sejf, Azure jako codzienne narzędzie pracy, wynika wprost z lekcji o transferze: chmura jest tania w przechowywaniu i przetwarzaniu na miejscu, a droga w wynoszeniu

danych na zewnątrz. Świadomość tego jednego mechanizmu kosztowego oszczędziła Zielonej więcej niż niejedna optymalizacja techniczna.

Mapa tej książki

Rozdział	Na jakie pytanie odpowiada
Pojęcia i AWS CLI	Jakie modele i pojęcia chmury trzeba znać i jak połączyć się z AWS z linii poleceń
S3: kubełki i dostęp	Jak przechowywać pliki w S3, kto ma do nich dostęp i jak je pobrać z Windows
Backup do S3	Jak trafia tam kopia zapasowa bazy danych i na czym polegają ograniczenia agenta backint
Azure i urządzenia	Jak wygląda codzienna praca w Azure oraz jak zarządzamy urządzeniami służbowymi i prywatnymi

Powiązane: Chmura: pojęcia, które trzeba znać zanim cokolwiek uruchomimy · Backup bazy do S3: agent backint i jego ograniczenia

Źródła: aws.amazon.com/about-aws/whats-new/2006/03/14/announcing-amazon-s3-a-simple-storage-service, aws.amazon.com/blogs/aws/amazon-ec2-beta, en.wikipedia.org/wiki/Microsoft_Azure, en.wikipedia.org/wiki/Time-sharing, learn.microsoft.com/azure, docs.aws.amazon.com/whitepapers/latest/aws-overview-security-processes/shared-responsibility-model.html