Z GŁOWĄ W CHMURZE

O MNIE

- Cześć jestem Szymon
- Mam 5 letnie doświadczenie jako architekt/inżynier chmury
- Obecnie pracuję jako Senior Cloud Engineer w firmie Bayer

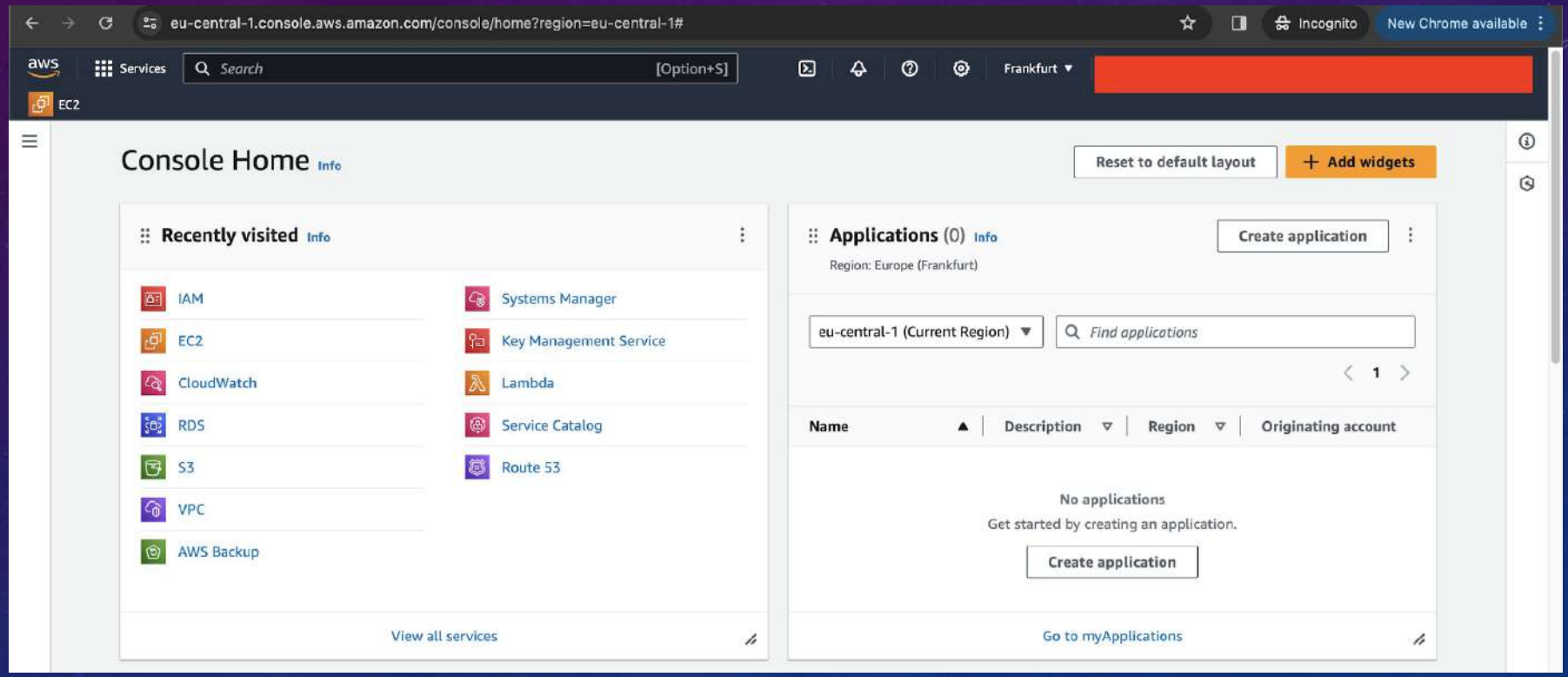
CZYM JEST CHMURA?

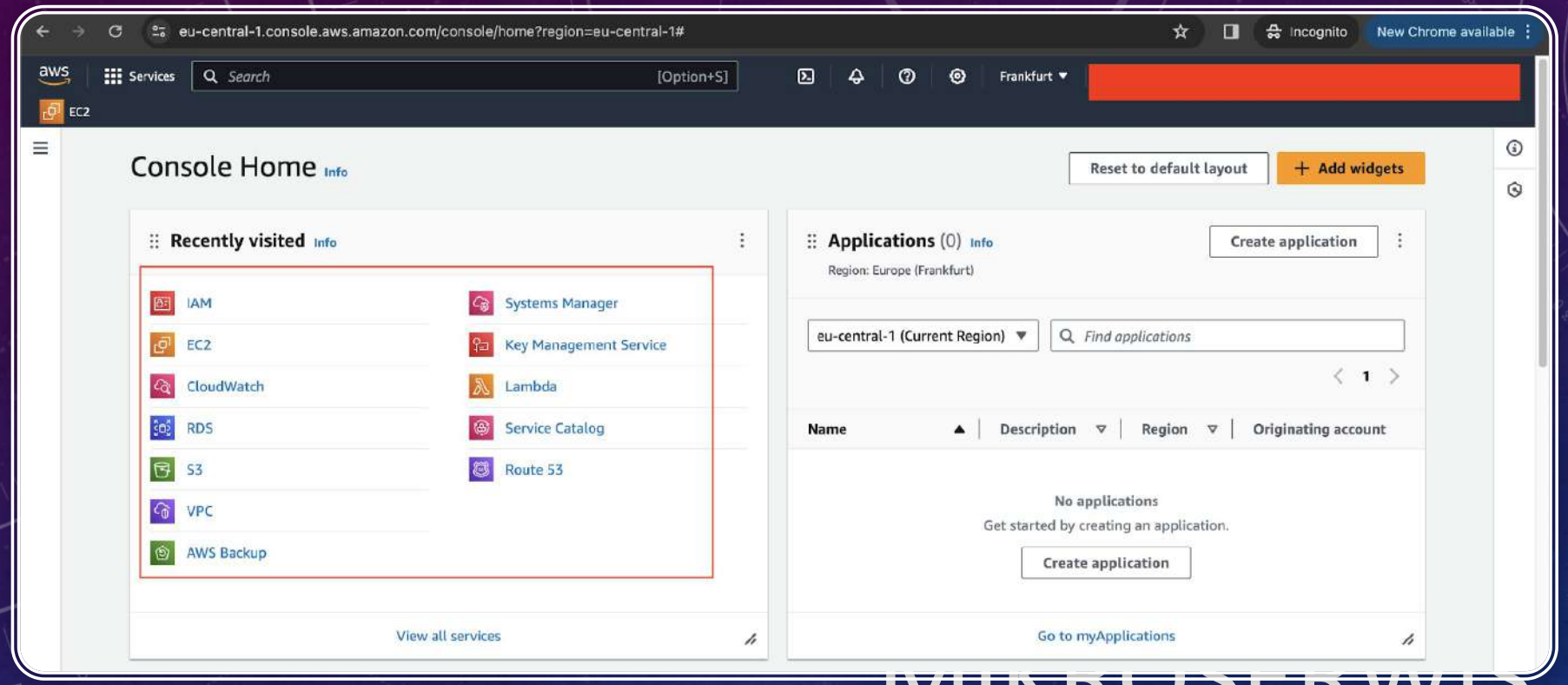
NAJWIĘKSI GRACZE

Źródło https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/


TO JEST CHMURA

TO TEŻ JEST CHMURA

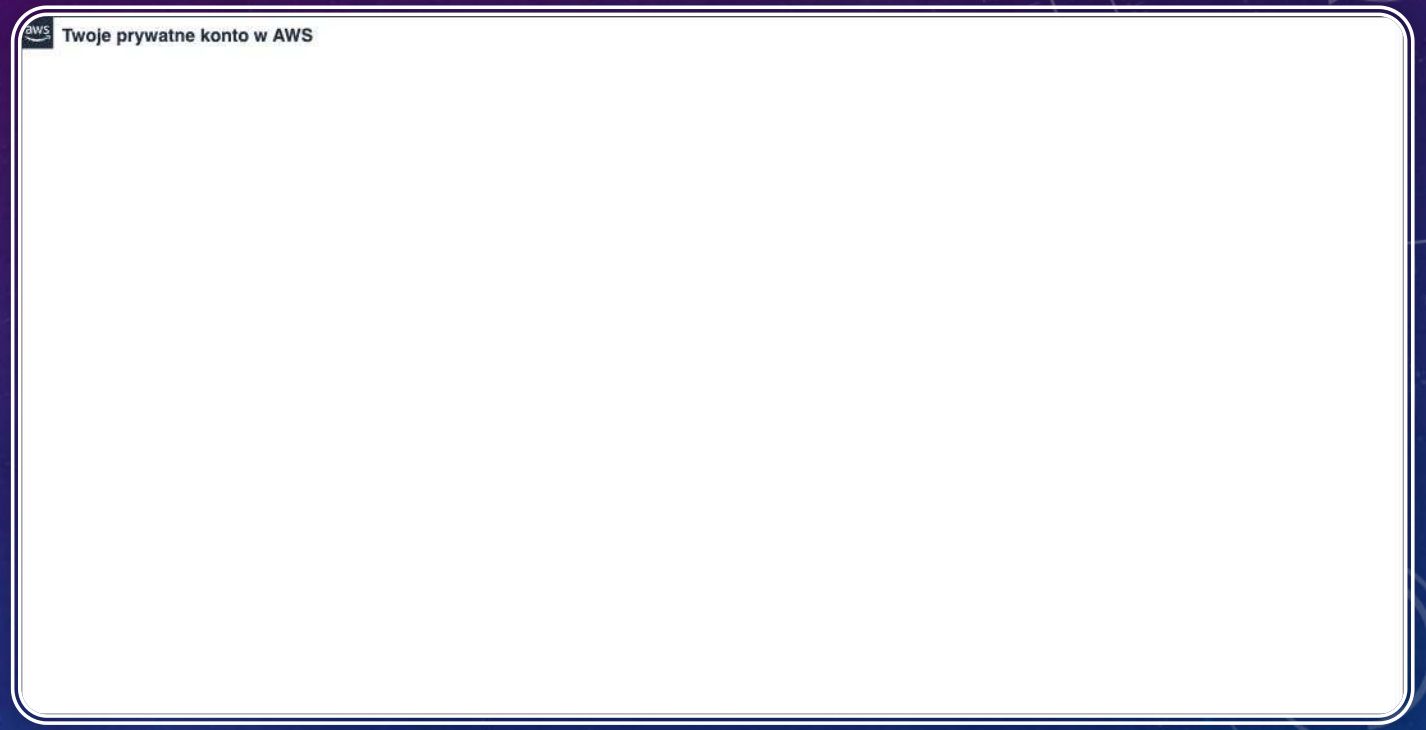




MIKROSERWIS Y

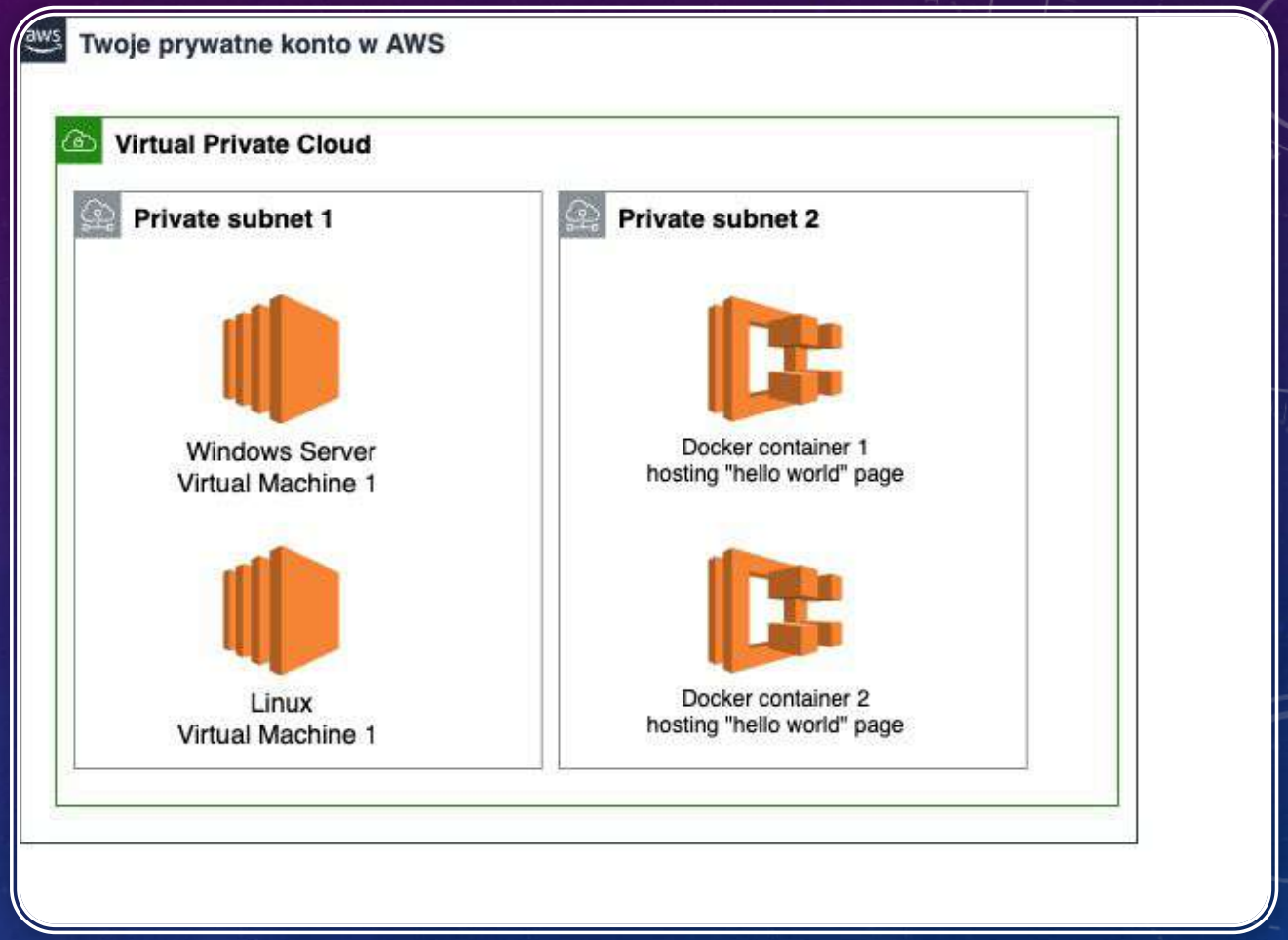
JAK MOGĘ ZACZĄĆ SWOJĄ PRZYGODĘ?

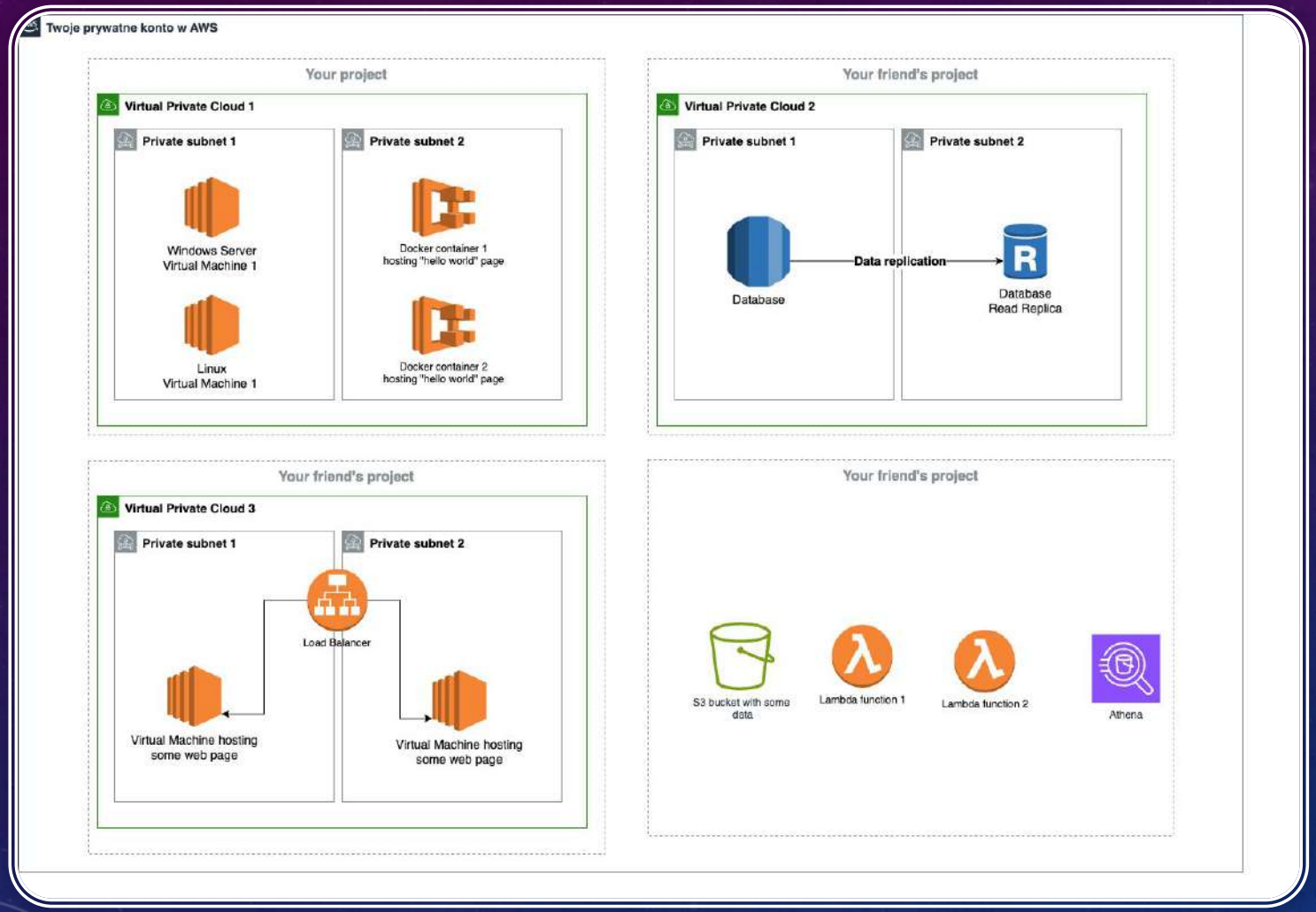
- Konto w chmurze może założyć każdy. Rejestracja jest podobna do tej na Facebooku tylko, że trzeba podać kartę kredytową.
- Na początku konto jest totalnie puste. Od Ciebie zależy jak je skonfigurujesz.
- Najpopularniejsze serwisy w chmurze często mają darmowy okres próbny.



TYDZIEŃ PÓŹNIEJ

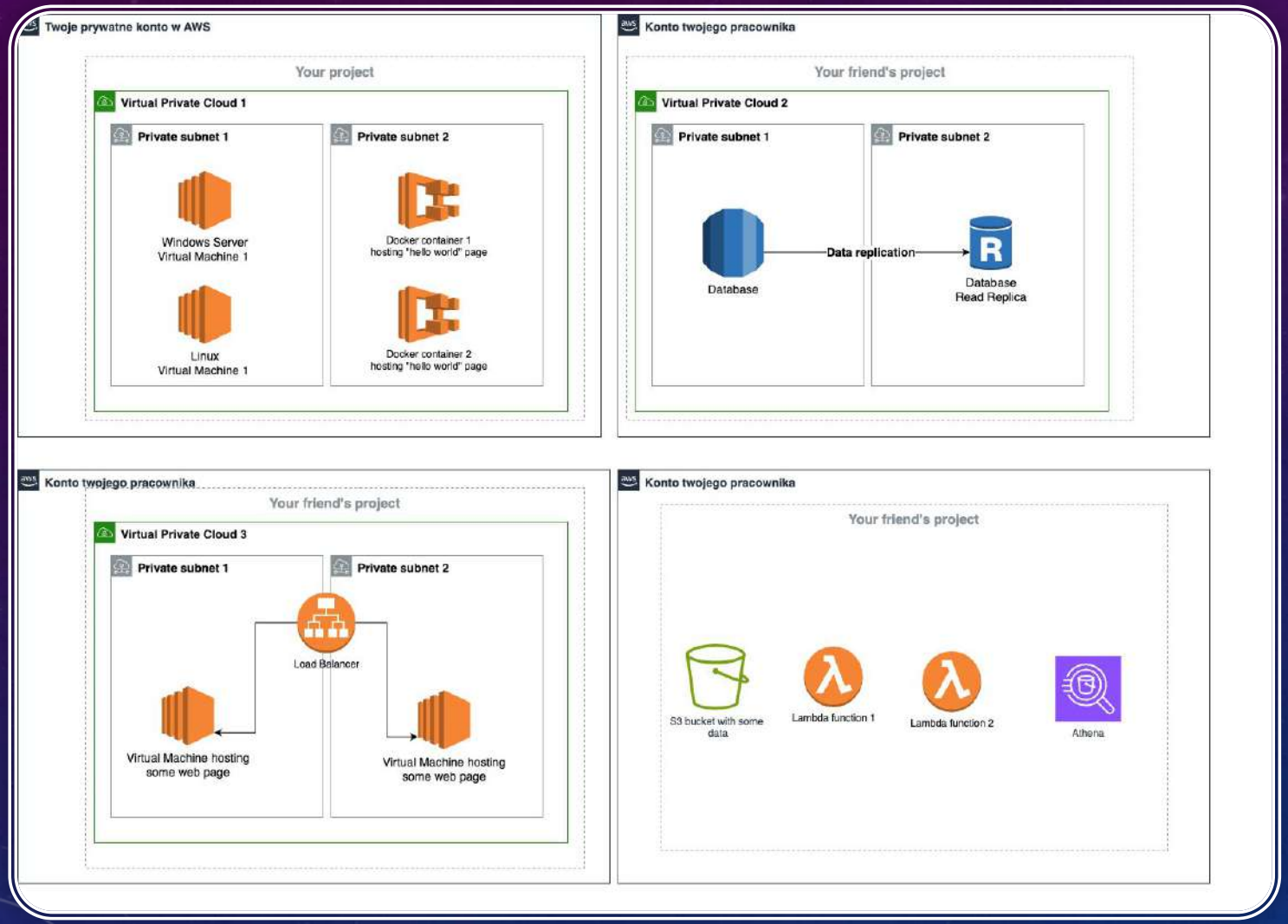
- Skonfigurowałeś/aś swoje pierwsze serwisy w AWS. Gratulacje!
- Używając przeglądarki “wyklikałeś/aś” dwie wirtualne maszyny używając mikroserwisu “EC2”.
- Używając przeglądarki “wyklikałeś/aś” dwia kontenery dockerowe używając serwisu “ECS”.





TAK CI SIĘ SPODOBAŁY MIKROSERWISY, ŻE ZAKŁADASZ WŁASNĄ FIRMĘ

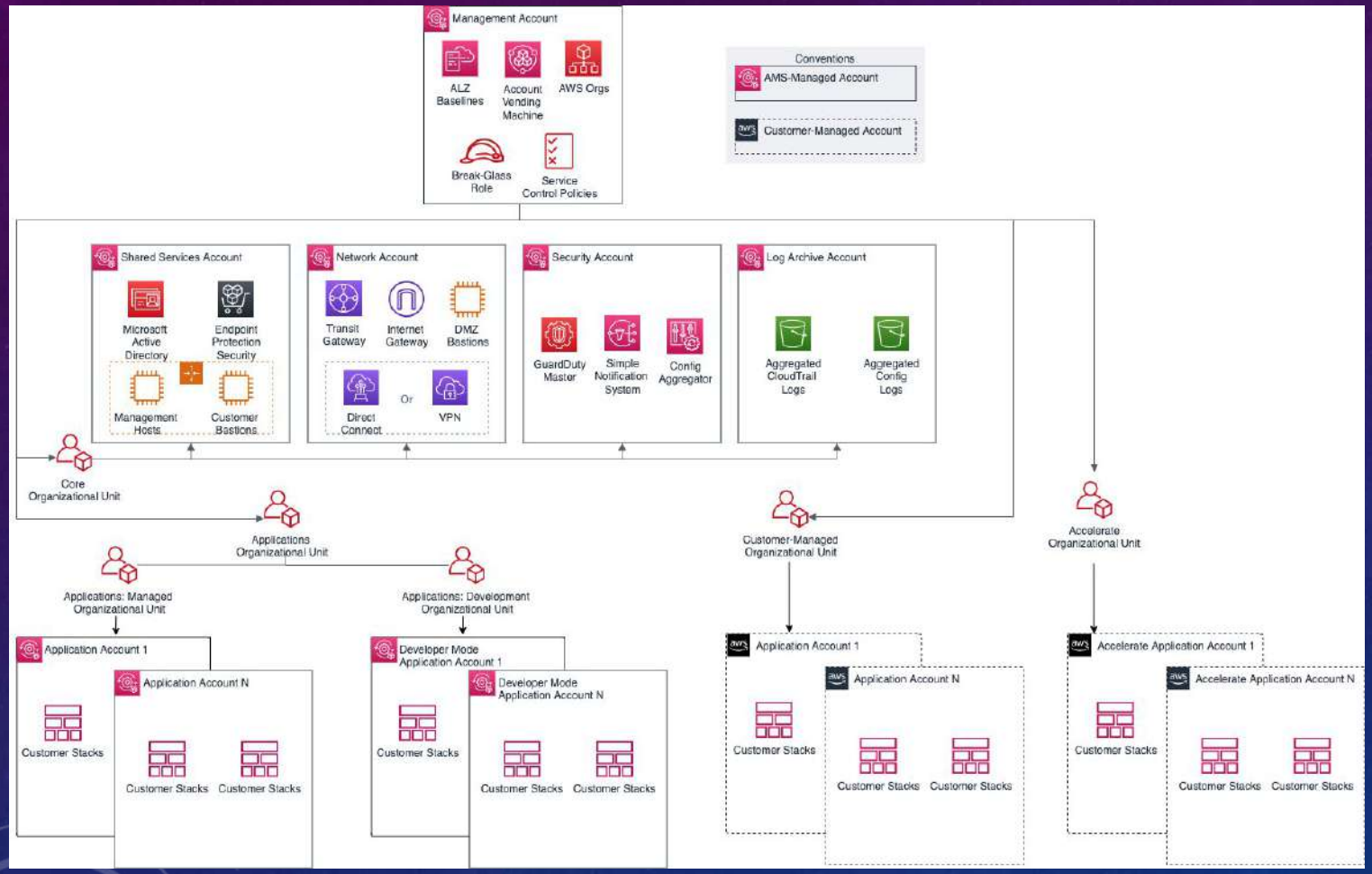
- Zatrudniłeś 10 osób i każdy zaczyna działać na twoim koncie.
- Robi się ciasno



POSTANAWIASZ, ŻE KAŻDY ZAŁOŻY WŁASNE KONTO W CHMURZE I DZIĘKI TEMU BĘDZIE LEPSZA ORGANIZACJA

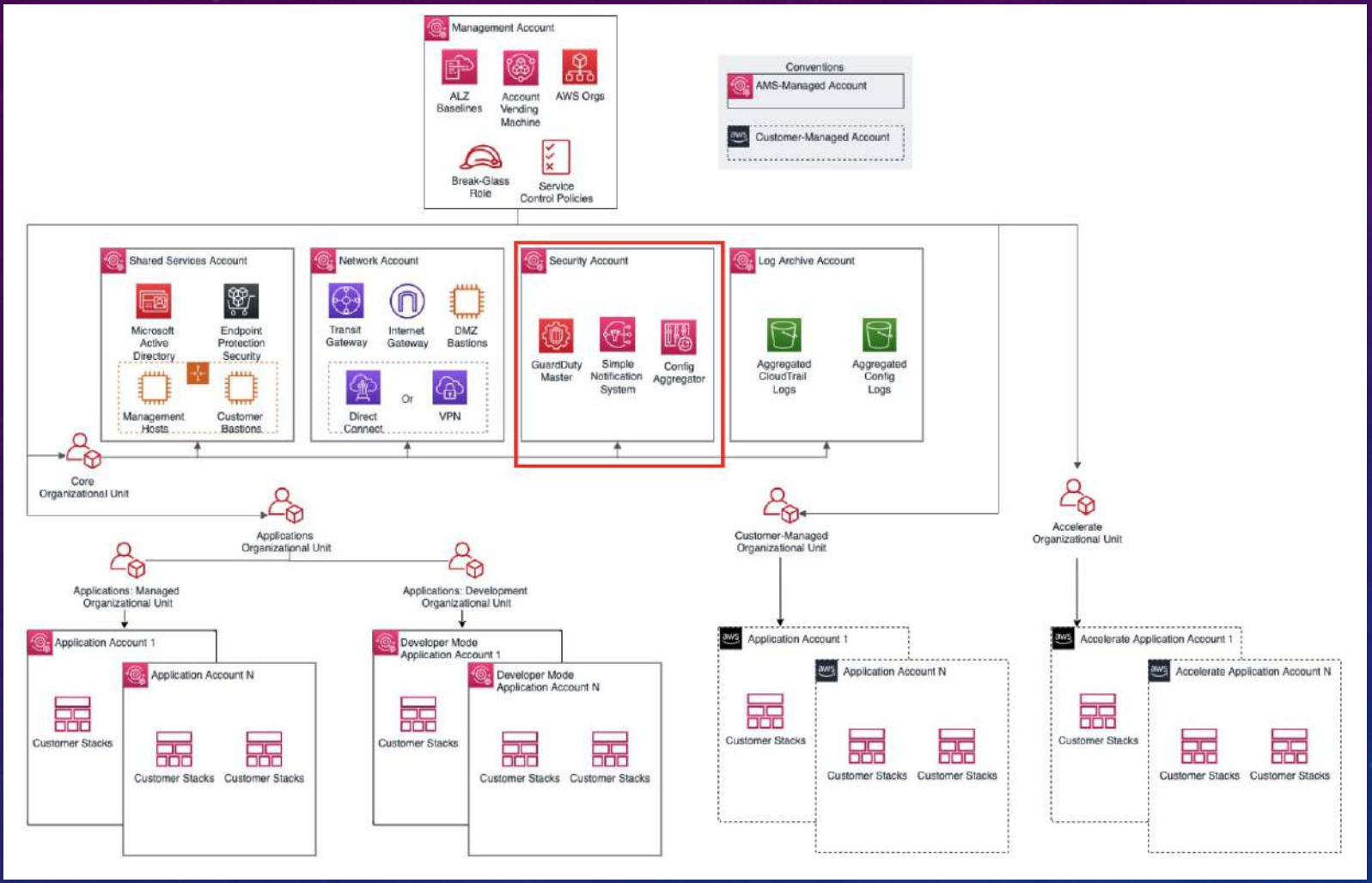
- Pierwszy problem jest taki, że każdy pracownik musi płacić za swoje konto w chmurze co im się nie podoba.
- Drugi problem jest taki, że projekty trudno jest ze sobą połączyć. Twój projekt i projekt twojego pracownika potrzebuje dodatkowej konfiguracji by Wasze mikroserwisy widziały siebie nawzajem.

LANDING ZONE – CZYLI OGROMNA SIEĆ RÓŻNYCH KONT W CHMURZE POŁĄCZONA ZE SOBĄ NA WIELU POZIOMACH



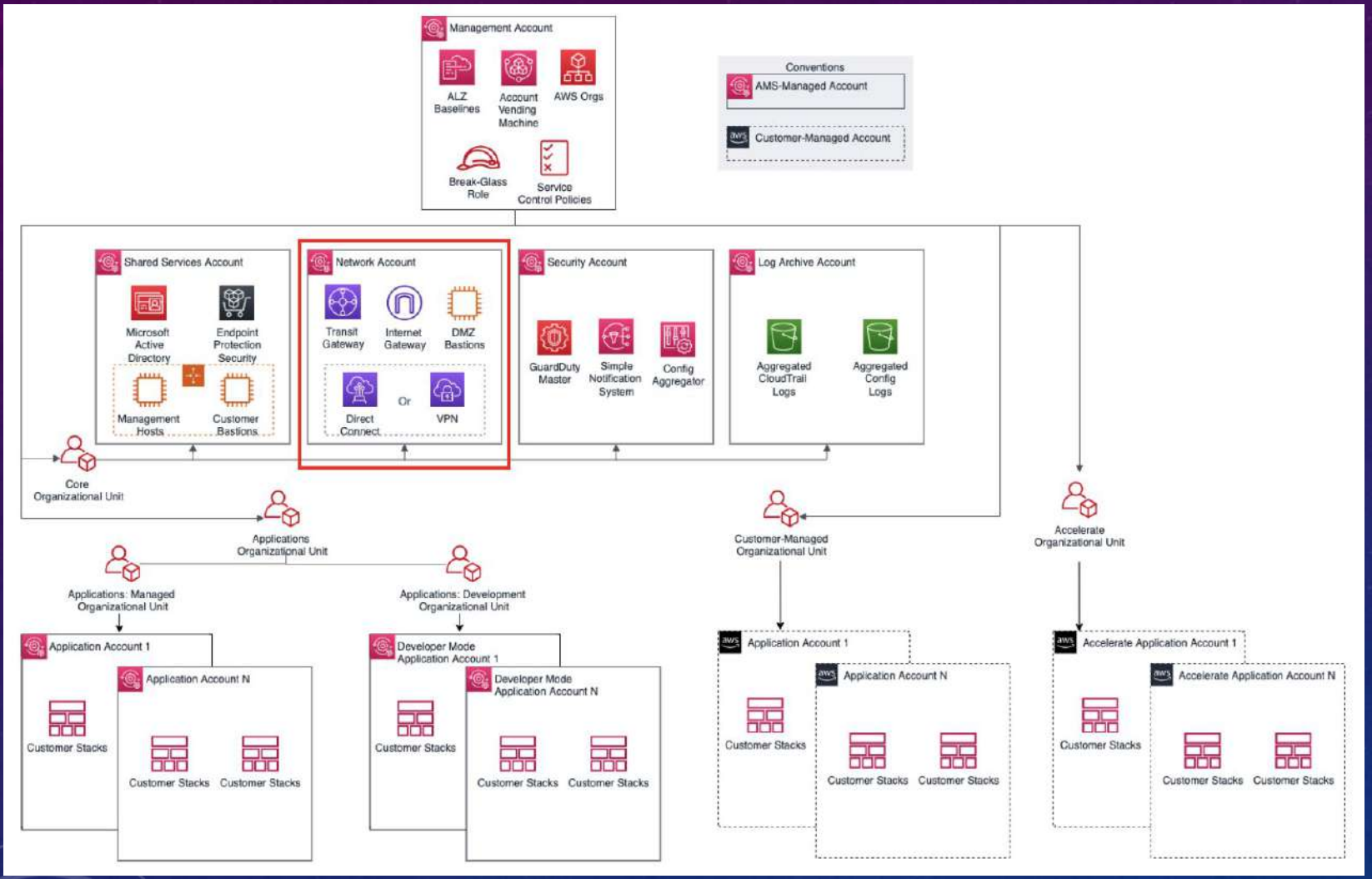
Landing zone łączy wszystkie konta danej firmy na wielu różnych poziomach:
- bezpieczeństwa
- sieciowym
- audytowym
- operacyjnym

ROLE W CHMURZE – SECURITY



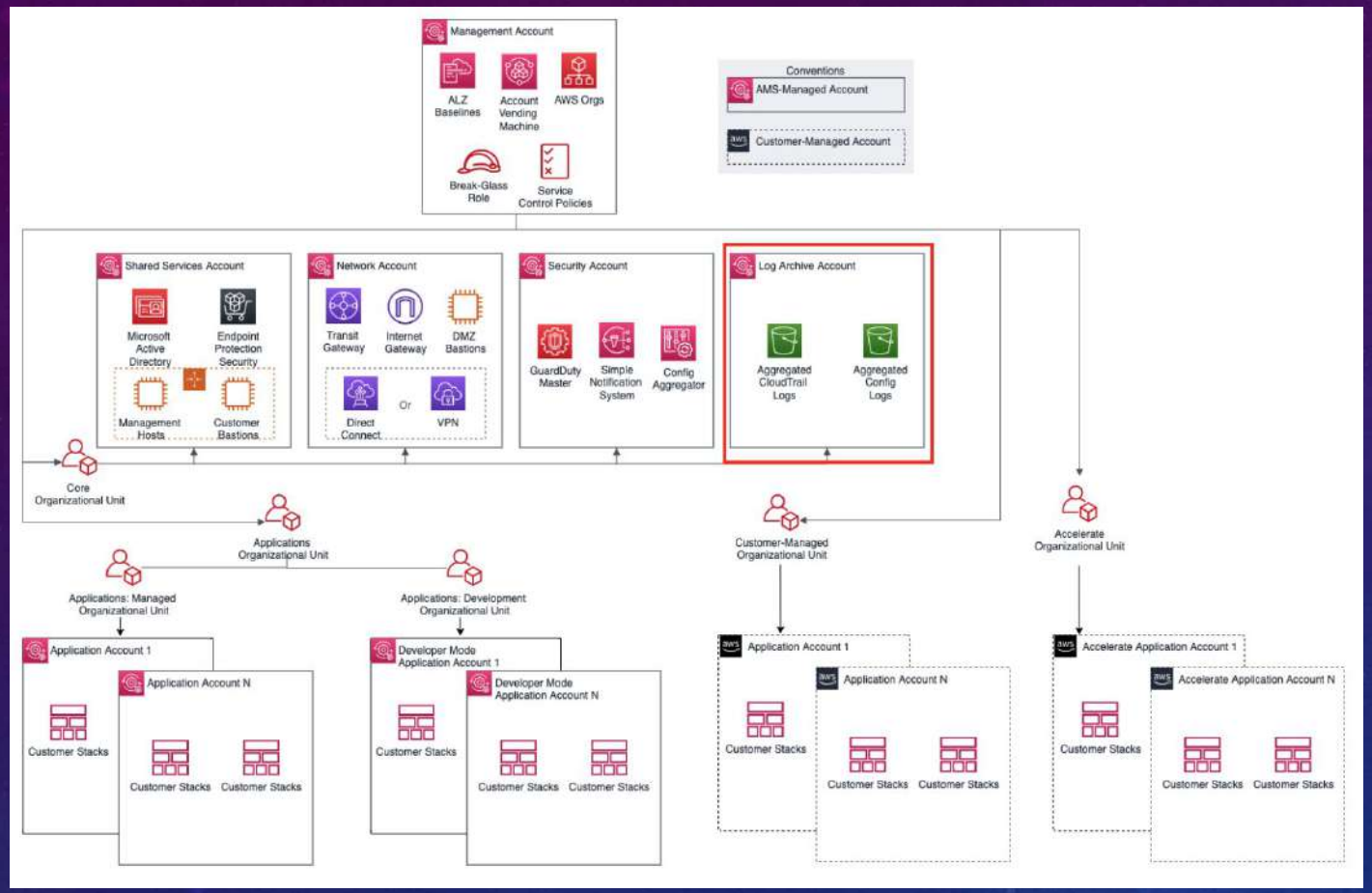
Zazwyczaj jedno z kont w chmurze przeznaczone jest wyłącznie do zarządzania bezpieczeństwem pozostałych kont w chmurze.
Specjaliści do spraw bezpieczeństwa:
- monitorują co dzieje się na innych kontach przy pomocy specjalnych mikroserwisów.
- ograniczają to co można a czego nie można robić na danych kontach w chmurze.

ROLE W CHMURZE – NETWORKING



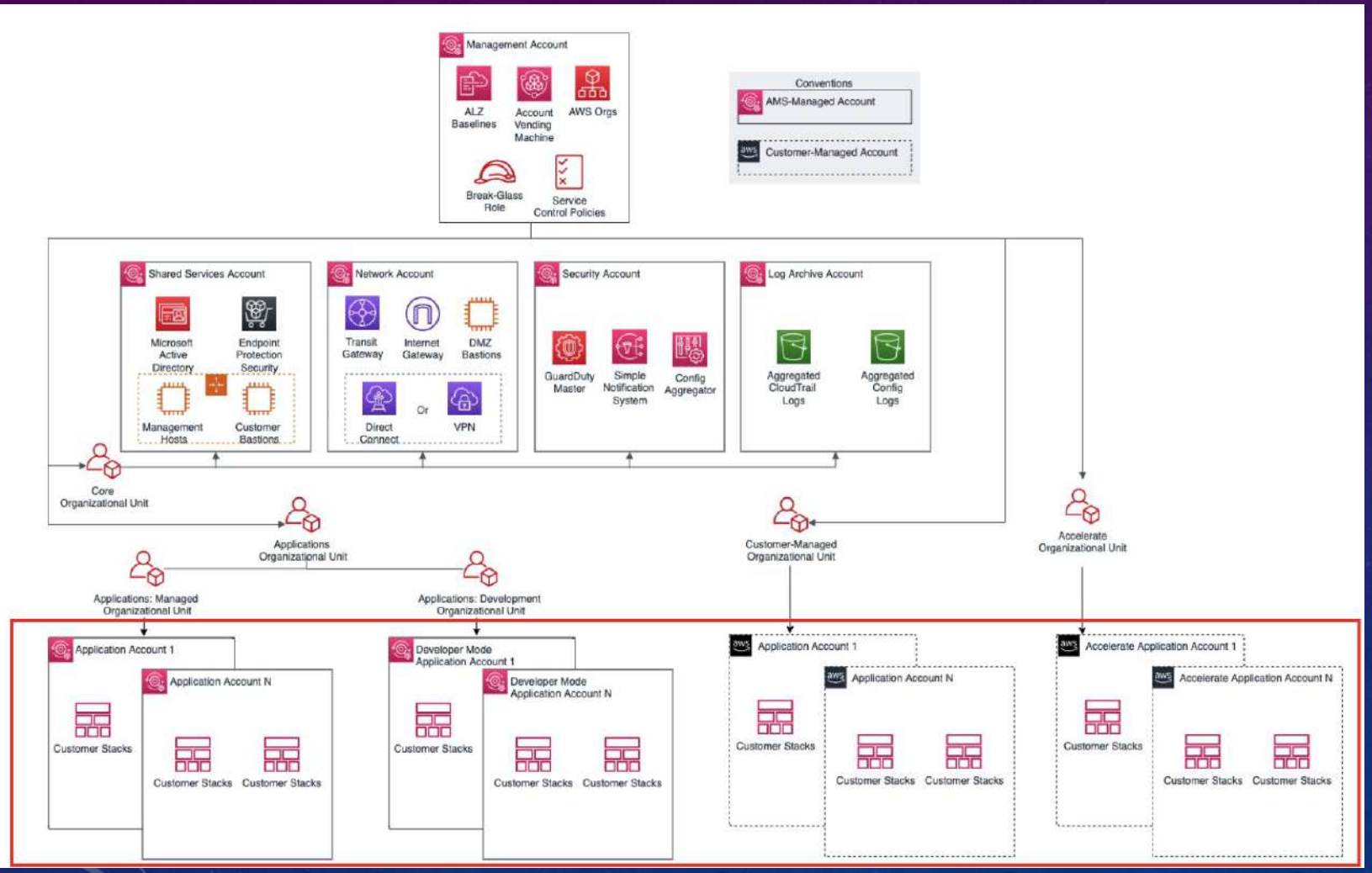
Zazwyczaj jedno z kont w chmurze przeznaczone jest wyłącznie do zarządzania siecią łączącą wszystkie konta w chmurze. Specjaliści do spraw sieciowych:
- przy pomocy specjalnych mikroserwisów definiują połączenia pomiędzy różnymi kontami w chmurze a nawet z lokalnym centrum danych.

ROLE W CHMURZE – AUDITOR



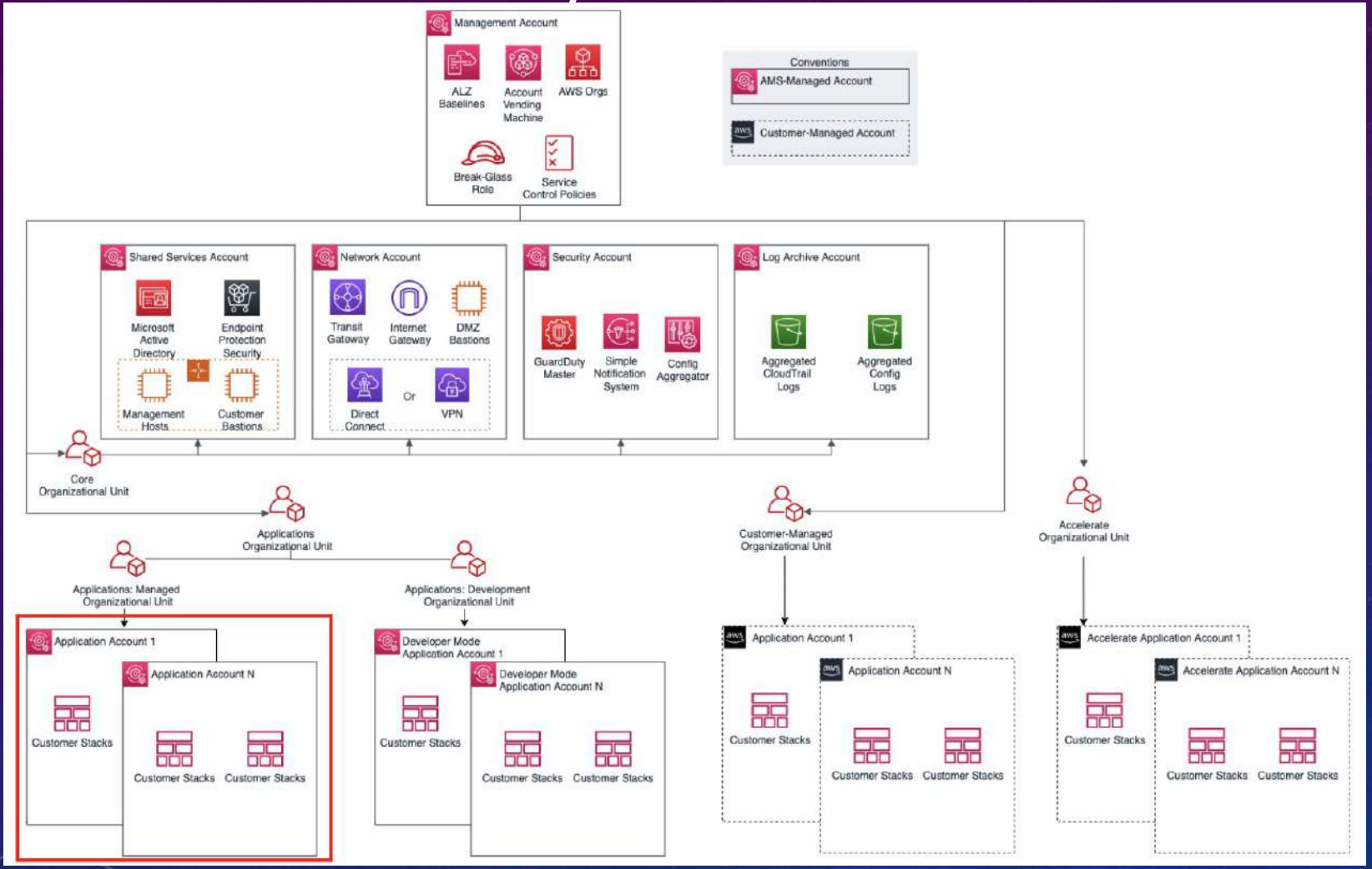
Zazwyczaj jedno z kont w chmurze przeznaczone jest wyłącznie do zarządzania logami które pokazują aktywność ze wszystkich innych kont. Jest to bardzo ważne, bo dzięki temu łatwo zobaczyć kto zrobił coś co naraziło firmę na jakiekolwiek ryzyko.
Specjaliści do spraw audytowych:
- zarządzają ogromną ilością logów
- tworzą reguły wyłapujące logi które wyglądają podejrzanie

ROLE W CHMURZE – DEVOPS



Specjaliści do spraw devops:
- współpracują z innymi zespołami i automatycznie wdrażają globalne rozwiązania w chmurze(globalne czyli na każdym koncie).
- udostępniają gotowe rozwiązania które inne konta w chmurze mogą bardzo łatwo wdrożyć bez znania szczegółów tego w jaki sposób one działają.

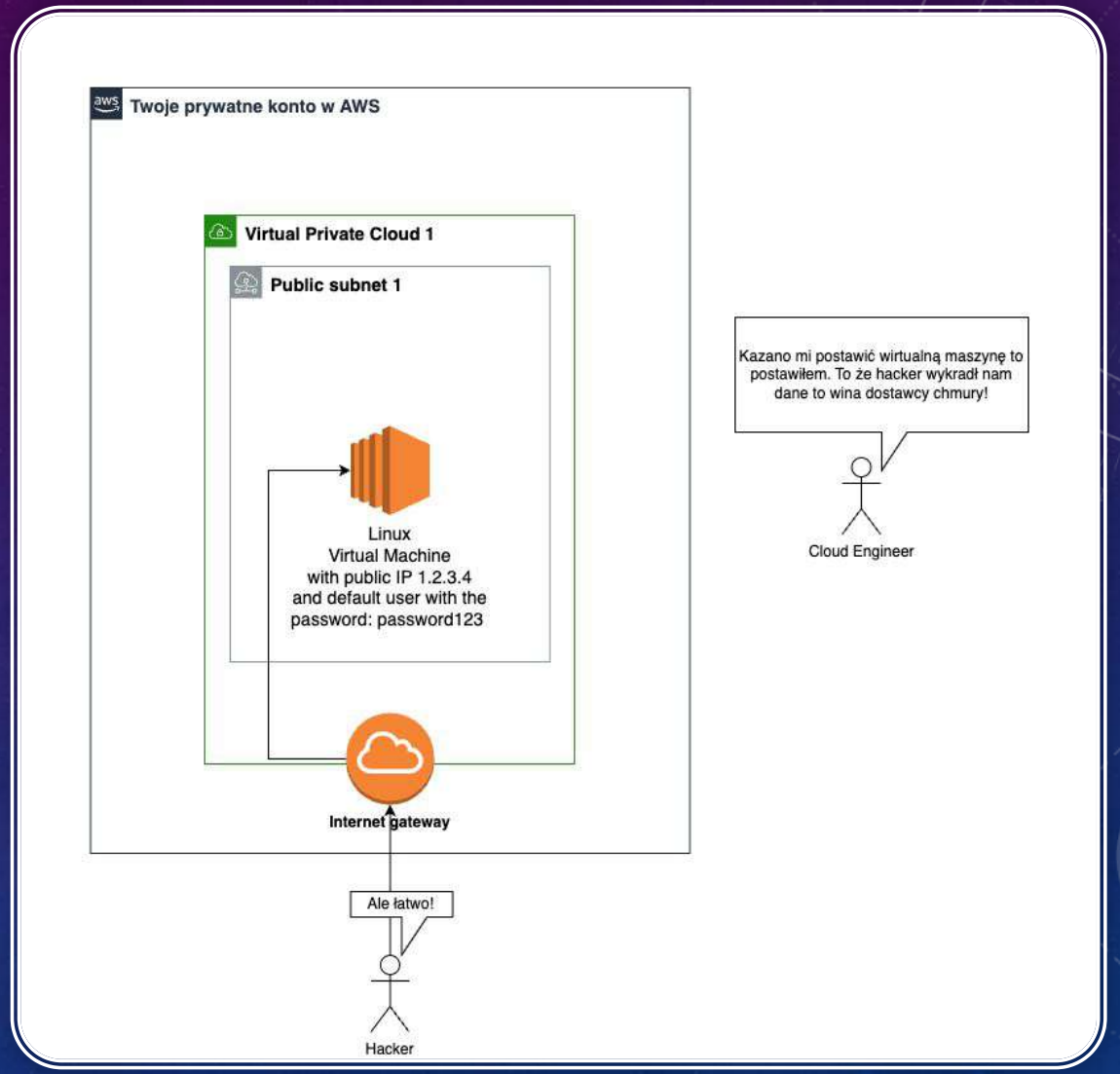
ROLE W CHMURZE – CLOUD ENGINEER/ARCHITECT



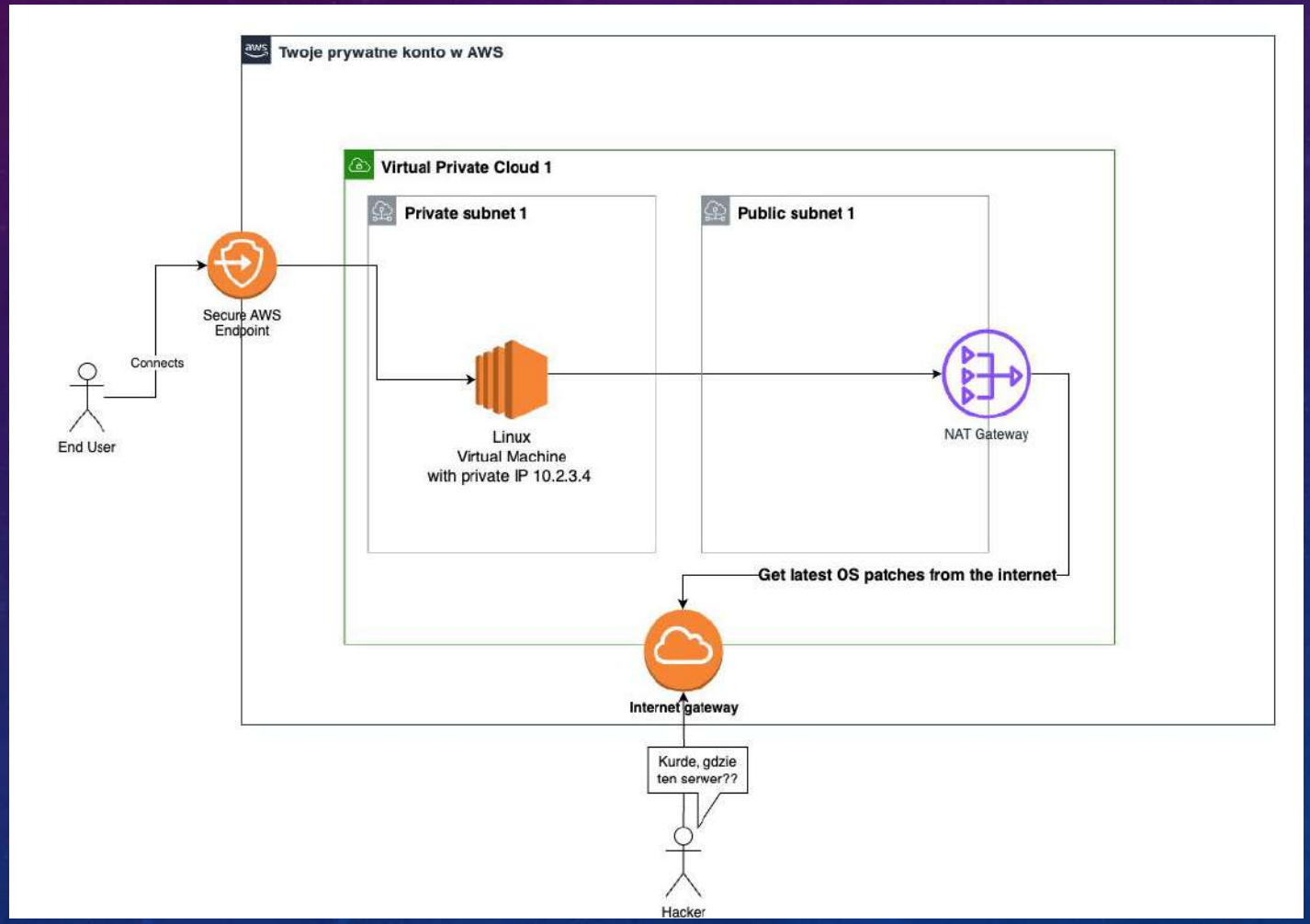
Specjaliści do spraw cloud engineer/architect:
- zwykle pracują nad konkretnymi projektami na pojedynczych kontach w chmurze.

MODEL WSPÓŁDZIELONEJ ODPOWIEDZIALNOŚCI

Model współdzielonej odpowiedzialności jest jedną z najważniejszych rzeczy o jakich musimy pamiętać kiedy konfigurujemy nasze mikroserwisy. Dostawca chmury dostarcza nam setki mikroserwisów ale to od nas zależy jak ich użyjemy.
To my jesteśmy odpowiedzialni za ich bezpieczną konfigurację.

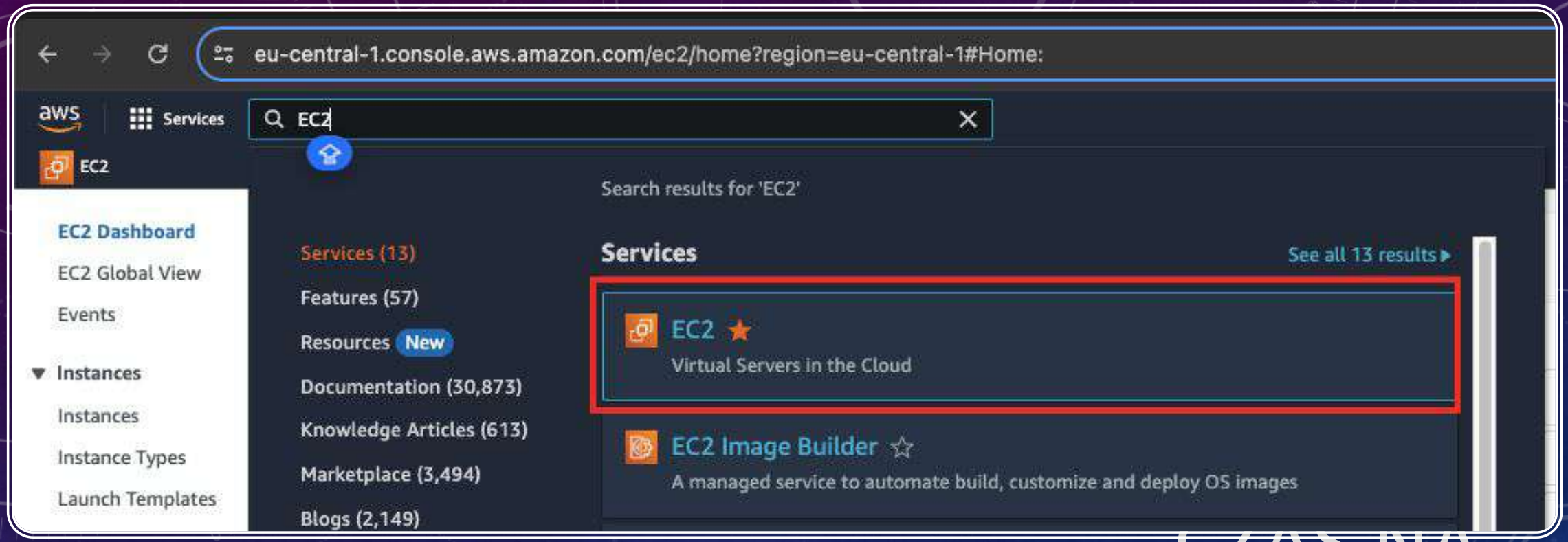


JAK TO POWINNO WYGLĄDAĆ

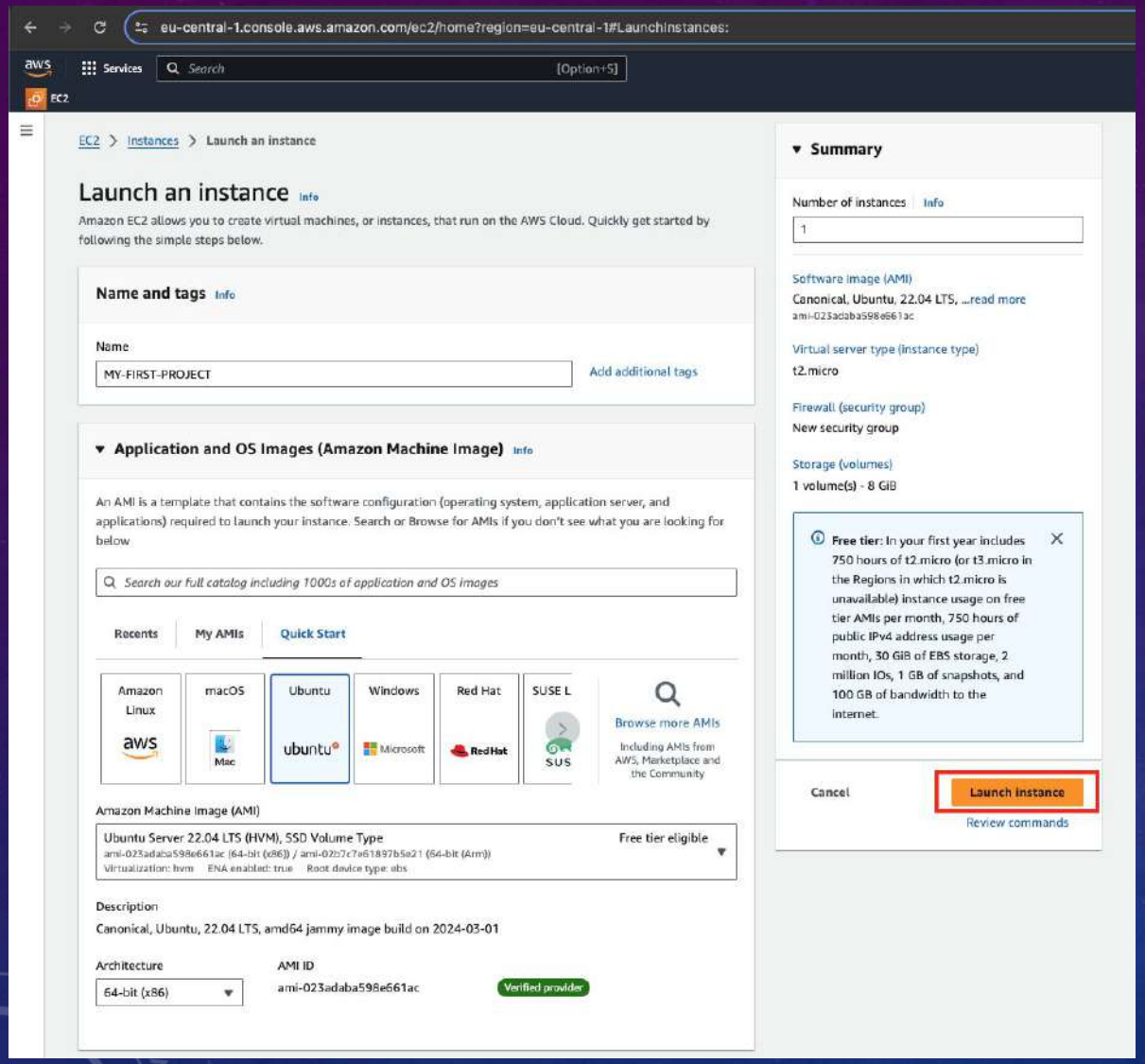


WŁAŚNIE ZOSTALIŚCIE CLOUD ENGINEEREM, GRATULACJE!

- Jako wasz pierwszy projekt poproszono was o dostarczenie wirtualnej maszyny z najnowszym systemem Ubutu. Proste? No pewnie, przecież obrazy z systemem Ubuntu są już w chmurze!

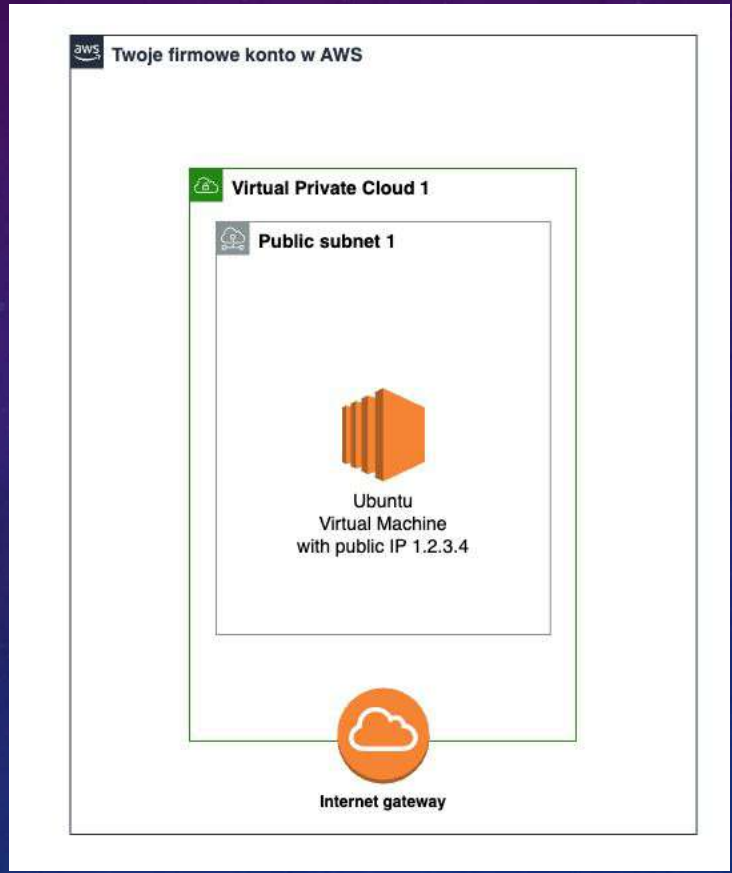


CZAS NA IMPLEMENTACJĘ



IDZIESZ JAK BURZA!

GOTOWE!



CZY NA PEWNO?

- Na maila dostajesz wiadomość od narzędzia skonfigurowanego przez zespół security gdzie natychmiast każą Ci zaszyfrować dyski twojej wirtualnej maszyny oraz ograniczyć do niej dostęp sieciowy.
- Ponadto na chacie na Teams'ach pisze do ciebie przedstawiciel zespołu security który pyta cię czy twoja maszyna wirtualna na pewno musi być publicznie dostępna i czemu nie jest prywatna.
- Dostajesz kolejnego maila od zespołu security w którym tym razem obrywa ci się za to, że nie używasz specjalnych obrazów Ubuntu które twoja firma dodatkowo zabezpieczyła w postaci oprogramowania skanującego OS i raportującego wszelkie ryzyka i niebezpieczeństwa.

ZAADRESOWAŁEŚ WSZYSTKIE INCYDENTY KTÓRE ZOSTAŁY ZGŁOSZONE NA POPRZEDNIM SLAJDZIE.
W KOŃCU MOŻESZ ODPOCZĄĆ. ALE CZY NA PEWNO?

- Zespół dla którego przygotowałeś wirtualną maszynę Ubuntu, teraz gdy nie jest już publiczna nie wie jak się do niej podłączyć i proszą cię o pomoc.
- Zespół dla którego przygotowałeś wirtualną maszynę Ubuntu oczekiwała, że będą się mogli do niej logować przy użyciu swoich firmowych loginów i haseł.

POKAZAŁEŚ ZESPOŁOWI W JAKI SPOSÓB POŁĄCZYĆ SIĘ DO PRYWATNEJ WIRTUALNEJ MASZYNY. DODAŁEŚ JĄ RÓWNIEŻ DO ACTIVE DIRECTORY I DZIĘKI TEMU ZESPÓŁ MOŻE LOGOWAĆ SIĘ DO NIEJ FIRMOWYMI HASŁAMI I LOGINAMI. W KOŃCU MOŻESZ ODPOCZĄĆ. ALE CZY NA PEWNO?

Zespół dla którego skonfigurowałeś wirtualną maszynę uważa, że to jest oczywiste, że będą chcieli się łączyć do bazy danych. Okazuje się, że baza danych do której chcą się połączyć jest w zupełnie innym regionie i musisz odtworzyć całe środowisko od nowa. Ponadto musisz skonfigurować bazę danych tak aby przyjmowała połączenia od wirtualnej maszyny Ubuntu którą tworzysz. Baza danych jest kontrolowana przez inny zespół i nie możesz sobie jej od tak zmienić. Piszesz maile i ustawiasz calle gdzie próbujesz wyjaśnić dlaczego potrzebujesz tego połączenia.

DŁUGO NIC NIE SŁYSZAŁEŚ OD ZESPOŁU DLA KTÓREGO POSTAWIŁEŚ SERWER UBUNTU.
W KOŃCU MOŻESZ ODPOCZĄĆ. ALE CZY NA PEWNO?

Mija pół roku i dostajesz wiadomość, że ktoś przez przypadek usunął jakiś super ważny plik I proszą cię żebyś przywrócił im maszynę wirtualną z backupu. Jakiego backupu? Przecież nie prosili żeby robić backupy?

Ponadto użytkownicy narzekają, że mają powiadomienia o tym, że system operacyjny nie ma najnowszych patch'y i update'ów.

SKONFIGUROWAŁEŚ AUTOMATYCZNE BACKUPY CODZIENNIE I SKONFIGUROWAŁEŚ AUTOMATYCZNĄ INSTALACJĘ NAJWAŻNIEJSZYCH PATCH'Y I UPDATE'ÓW. W KOŃCU MOŻESZ ODPOCZĄĆ. ALE CZY NA PEWNO?

Okazuje się, że wirtualna maszyna Ubuntu którą postawiłeś dla zespołu który cię o nią prosił służyła im jako POC. Teraz POC się skończyło i gotowi są iść na produkcję. Zanim to się jednak stanie, serwer musi przejść audyt na dodatkowym środowisku gdzie audytor oceni czy spełnia on wszystkie wymagania. Okazuje się, że jest to aplikacja krytyczna.

POSTAWIŁEŚ DWA NOWE ŚRODOWISKA – QUALITY I PRODUKCJĘ.
W KOŃCU MOŻESZ ODPOCZĄĆ. ALE CZY NA PEWNO?

Audytor zauważył, że nie widzi żadnego monitoringu aplikacji działającej na wirtualnej maszynie którą postawiłeś. Aplikacja nie przejdzie testów dopóki nie dodasz alarmów które włączą się gdy zabraknie miejsca na dysku, serwerowi zabraknie pamięci RAM oraz gdy zużycie procesora będzie zbyt wysokie przez określoną ilość czasu.

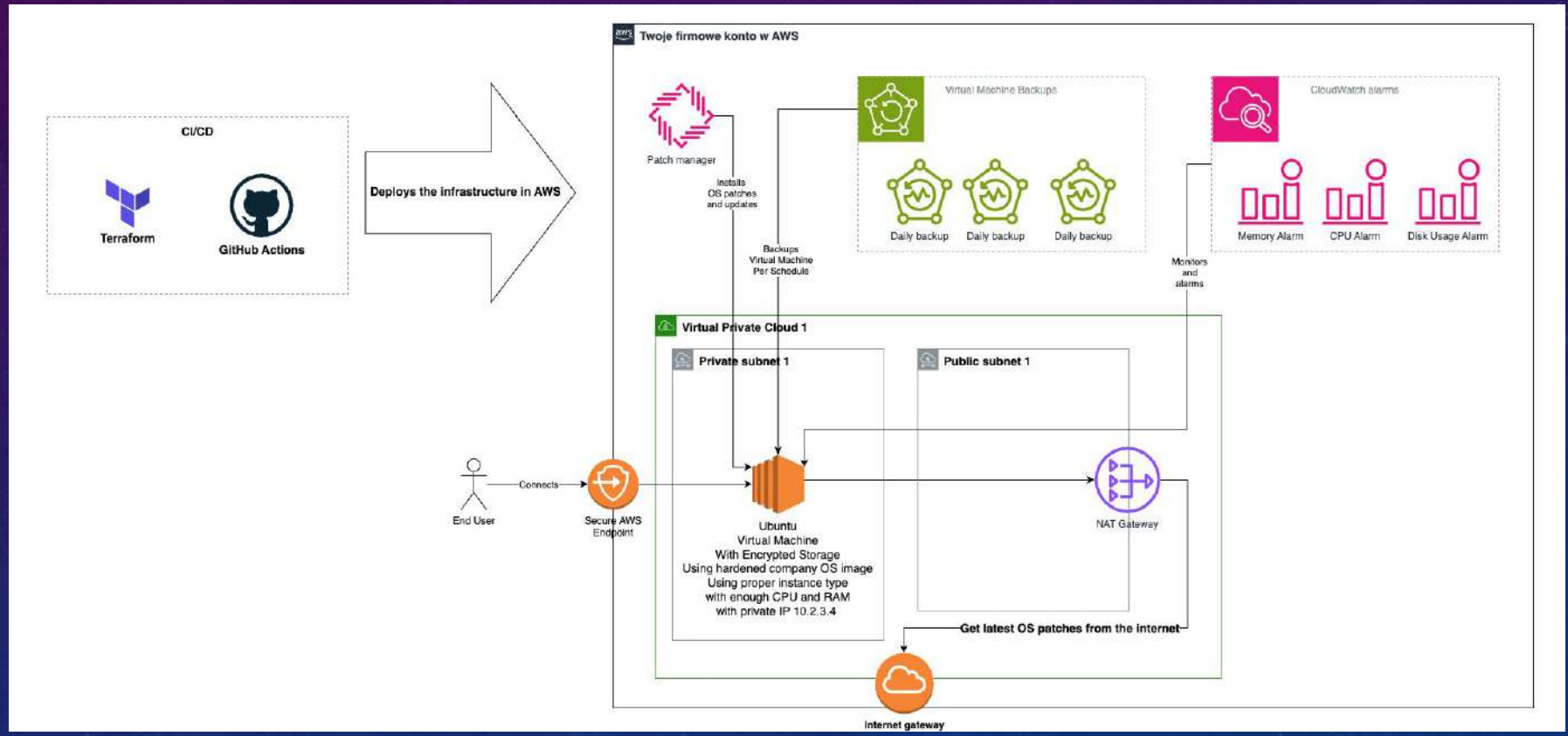
DODAŁEŚ ALARMY.
W KOŃCU MOŻESZ ODPOCZĄĆ. ALE CZY NA PEWNO?

Alarmy włączyły się jak tylko zostały przez ciebie stworzone. Wirtualna maszyna którą stworzyłeś jest za słaba by obsłużyć zainstalowaną na niej aplikację. Musisz ją zmienić na mocniejszy model - dodać więcej pamięci oraz mocy obliczeniowej procesora.

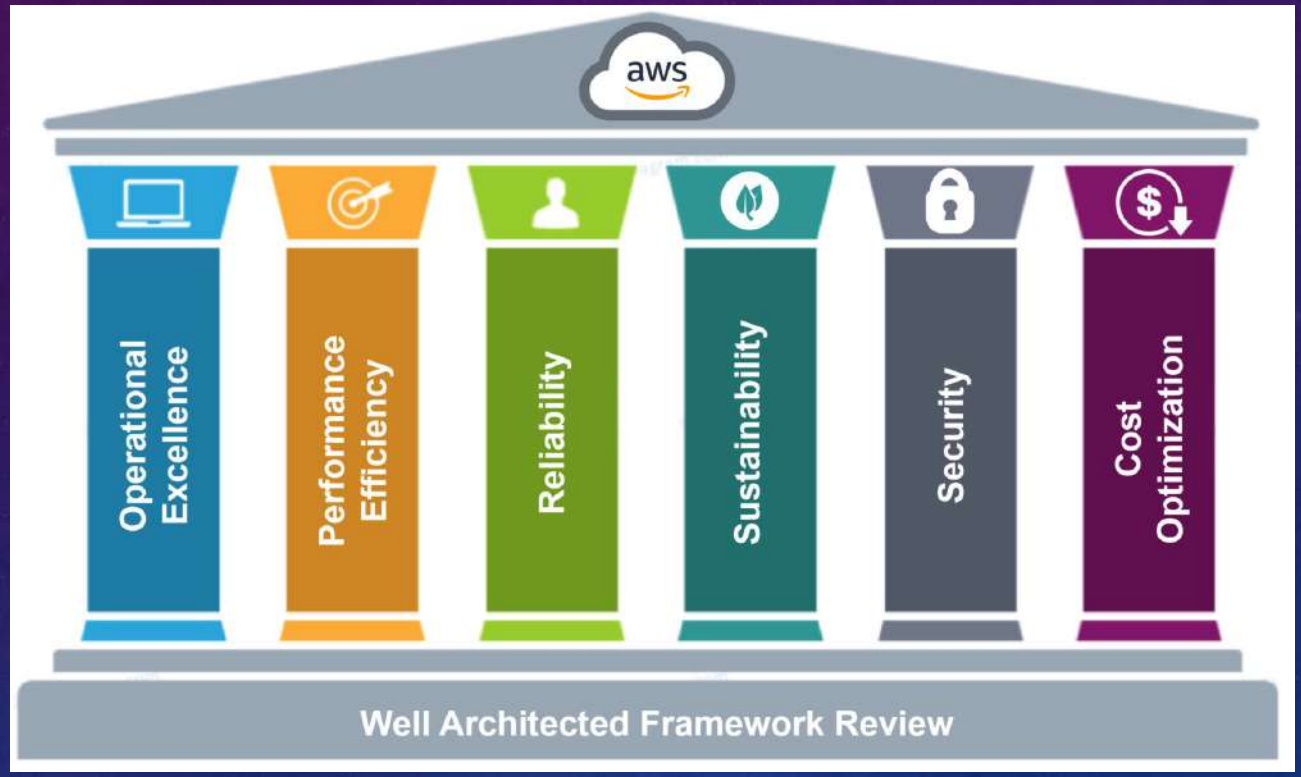
ZMIENIŁEŚ TYP INSTANCJI NA MOCNIEJSZY NA WSZYSTKICH ŚRODOWISKACH – DEV, QUALITY I PROD. W KOŃCU MOŻESZ ODPOCZĄĆ. ALE CZY NA PEWNO?

Inny zespół usłyszał, że potrafisz robić świetne maszyny wirtualne. Tak się składa, że potrzebują oni identycznej konfiguracji jak ta którą tworzyłeś na poprzednich 10 slajdach.
Robi ci się niedobrze na myśl, że musisz znów wyklikać wszystkie te rzeczy w przeglądarce.
Twój szloch usłyszał twój kolega Łukasz który tak się składa jest bardzo doświadczonym architektem.
Łukasz mówi ci, że istnieją technologie które bardzo ułatwiają tworzenie i ponowne użycie mikroserwisów w chmurze. Łukasz pokazuje ci jak przyjemne staje się tworzenie projektów i infrastruktury przy użyciu programu „Terraform” oraz systemu kontroli wersji GitHub. Czujesz, że poznajesz świat na nowo.

DRUGĄ MASZYNĘ WIRTUALNĄ Z PEŁNĄ KONFIGURACJĄ STWORZYŁEŚ PRZY UŻYCIU KODU. WSZYSCY SĄ POD WRAŻENIEM TEGO JAK BARDZO SIĘ ROZWINĄŁEŚ.

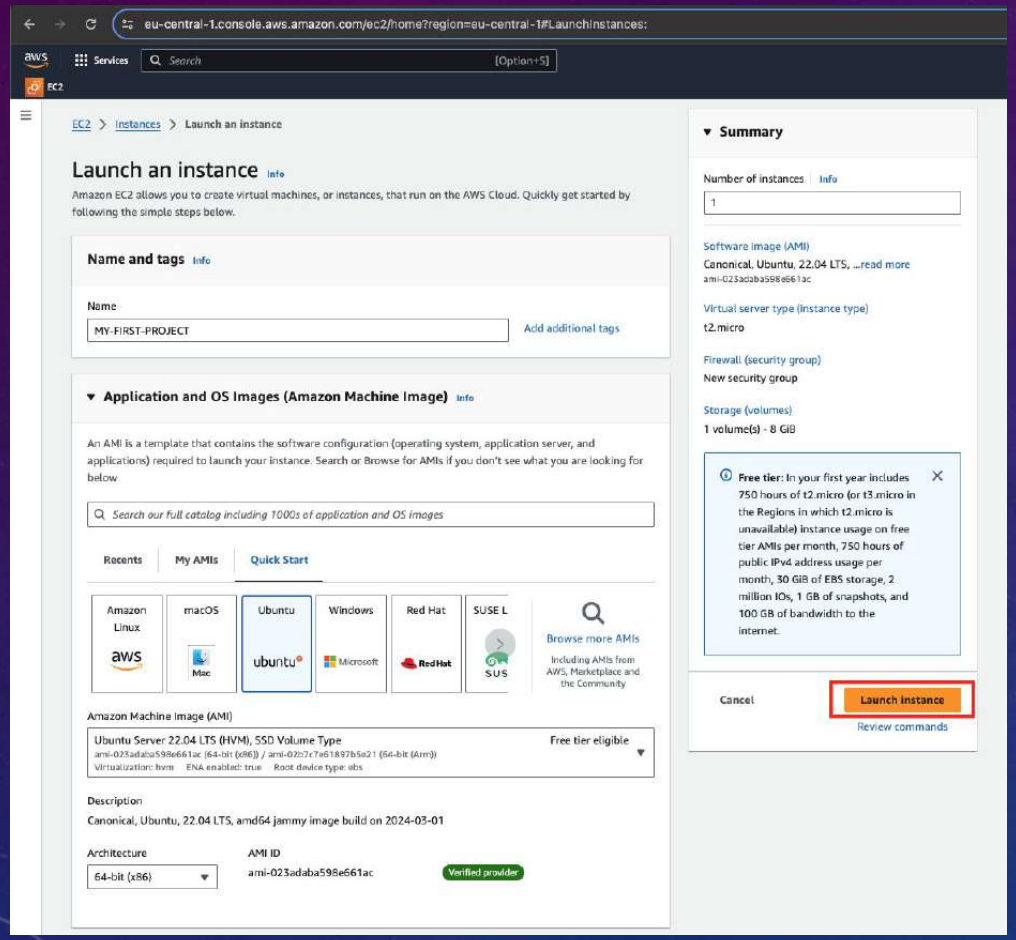


WELL ARCHITECTED FRAMEWORK



Wskazówki którymi powinno kierować się podczas projektowania infrastruktury w chmurze.

CLICKOPS VS INFRASTRUCTURE AS A CODE



virtual_machine.tf > resource "aws_instance" "my_first_project" > instance_type

```hcl
resource "aws_instance" "my_first_project" {

  #Company hardened image
  ami                  = "ami-xxxxxxxxxx"
  #Adjusted instance type with enough CPU and Memory
  instance_type        = "r7i.xlarge"
  #SSH KEY PAIR
  key_name             = aws_key_pair.my_first_project_ssh_key.key_name
  availability_zone    = module.vpc.private_subnet1_az
  monitoring           = true
  iam_instance_profile = aws_iam_instance_profile.project_ec2_profile.name
  ebs_optimized        = true

  metadata_options {
    http_endpoint = "enabled"
    http_tokens   = "required"
  }

  root_block_device {
    volume_size           = 200
    volume_type           = "gp3"
    #ENCRYPTION ENABLED
    encrypted             = true
    delete_on_termination = false

    tags = {
      Name = "root-volume"
    }
  }

  tags = {
    Name                  = "MY-FIRST-PROJECT"
    env                   = var.env
  }


  lifecycle {
    prevent_destroy = true
  }

}
```

Najczęstsze typy projektów w chmurze (moja subiektywna ocena)