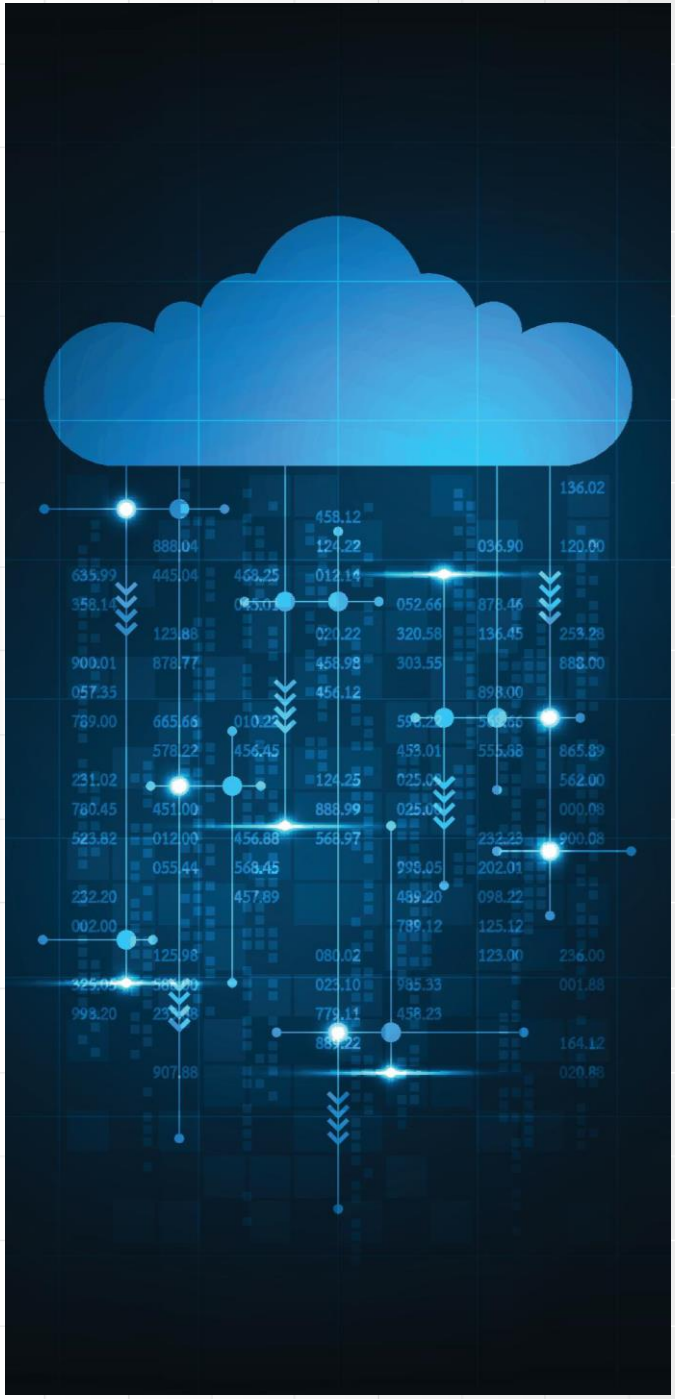


Programowanie w chmurze

Rafał Palak

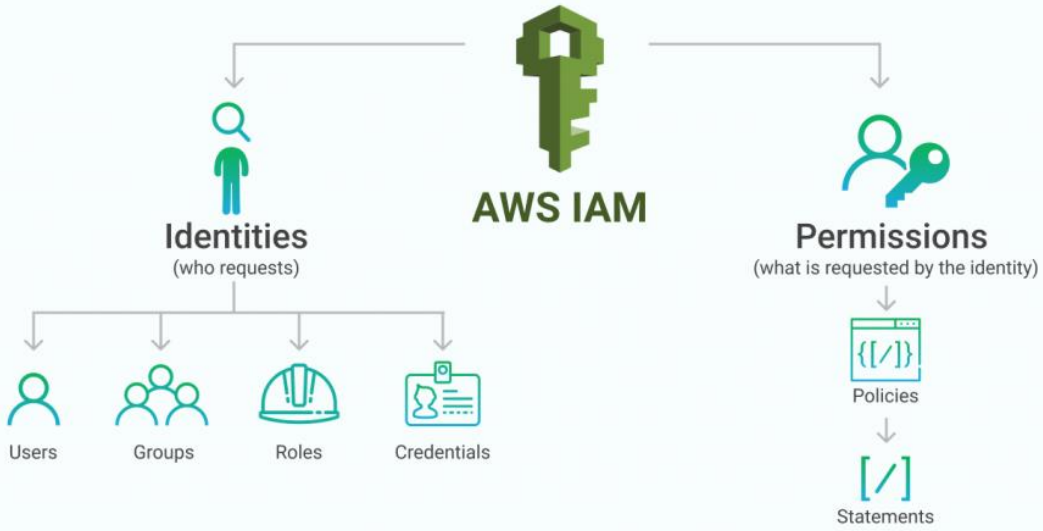
Politechnika Wrocławska

Wrocław
University
of Science
and Technology

Najistotniejsze zagadnienia

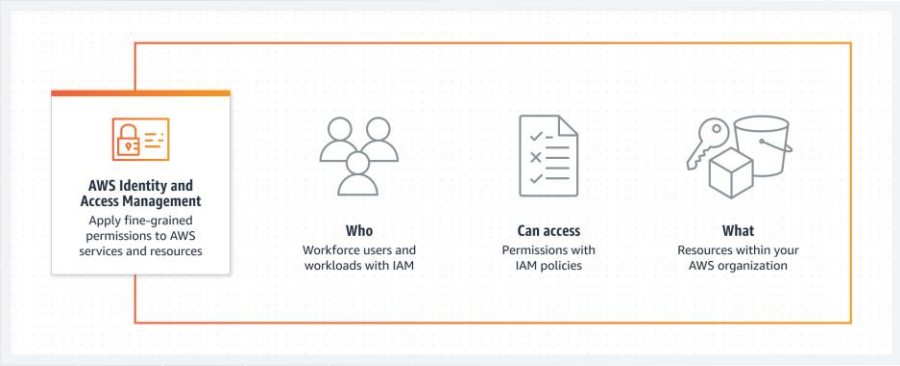
AWS Identity and Access Management (IAM) [1]

- Usługa sieciowa do bezpiecznego kontrolowania dostępu do zasobów AWS. Umożliwia tworzenie i kontrolowanie usług uwierzytelniania użytkowników lub ograniczanie dostępu do określonego zestawu osób korzystających z zasobów AWS.
- Obejmuje stosowanie kontroli dla użytkowników, którzy potrzebują dostępu do zasobów obliczeniowych



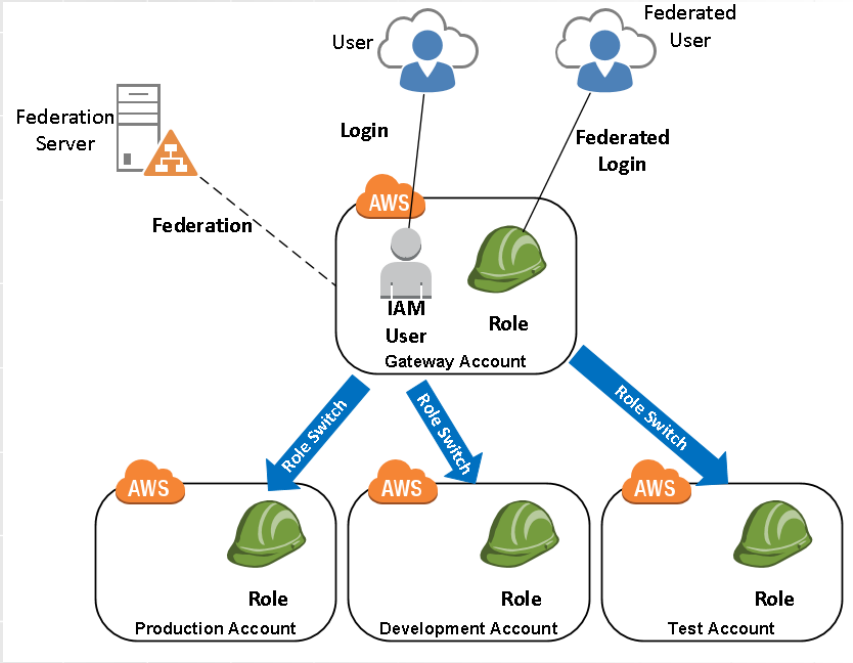
Użytkownik [1]

- Podmiot, tworzony w AWS, aby reprezentować osobę lub aplikację, używany do interakcji z AWS.
- Użytkownik w AWS składa się z nazwy i poświadczeń.
- Może to być rzeczywista osoba będąca użytkownikiem lub aplikacja będąca użytkownikiem
- Dzięki IAM możliwe jest bezpiecznie zarządzanie dostępem do usług AWS, tworząc nazwę użytkownika IAM dla każdego pracownika w organizacji



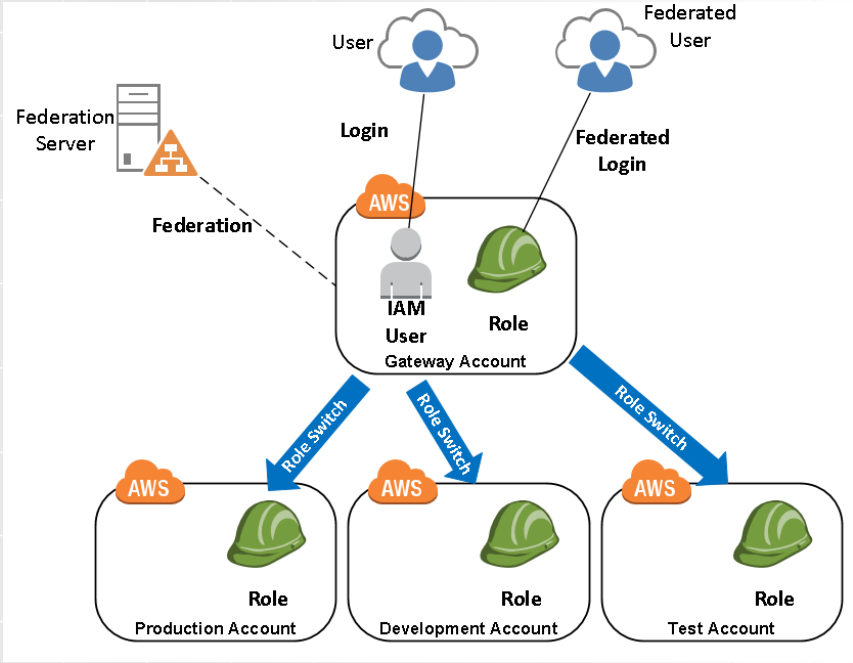
Rola [1]

- Tożsamość uprawnień, która ma określone uprawnienia
- Rola to zestaw uprawnień, które definiują, jakie działania są dozwolone i zabronione przez jednostkę w konsoli AWS
- Podobna do użytkownika, ponieważ może uzyskać do niego dostęp dowolny rodzaj podmiotu (osoba lub usługa AWS)
- Uprawnienia ról są tymczasowymi poświadczeniami



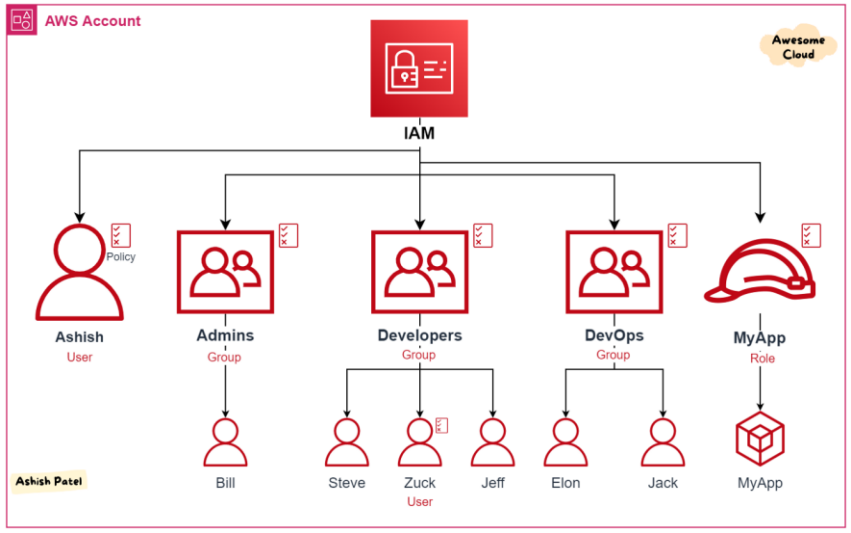
Rola [2]

- Użytkownik IAM może "przyjąć" rolę, co oznacza tymczasowe uzyskanie uprawnień określonych w tej roli. To umożliwia użytkownikowi wykonywanie zadań, na które jego osobiste konto IAM nie ma uprawnień.
- Rola może być przekazana usługom AWS np. EC2, aby umożliwić im dostęp do innych zasobów AWS bez konieczności wbudowywania stałych poświadczeń.
- Role mogą być używane do udzielania dostępu między różnymi kontami AWS. To oznacza, że użytkownik z jednego konta AWS może przyjąć rolę na innym koncie AWS, aby uzyskać tam dostęp do zasobów.



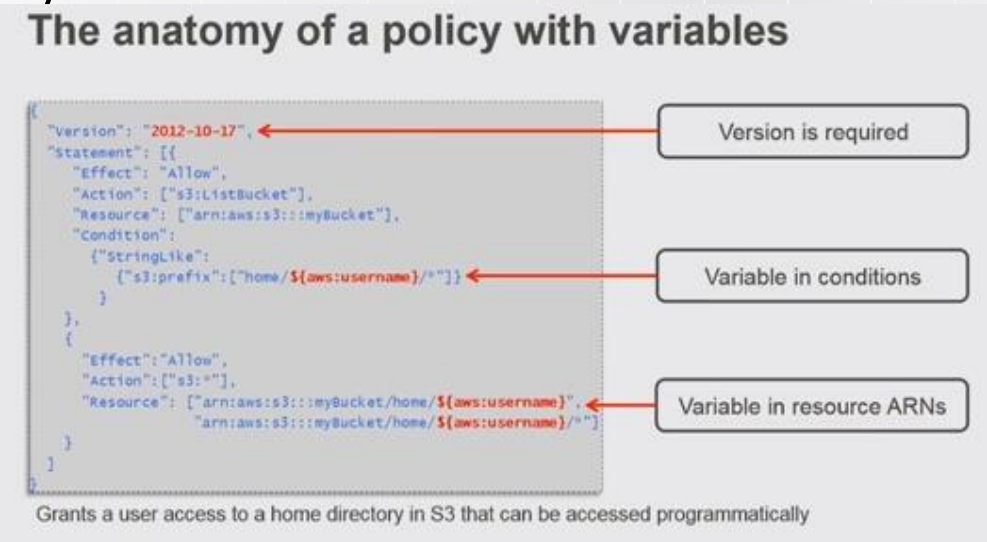
Grupa

- Zbiór uprawnień dla użytkowników
- Grupy umożliwiają określenie uprawnień dla wielu użytkowników
- Zmiany w uprawnieniach dla grupy, są automatycznie stosowane do wszystkich użytkowników w grupie
- Dodanie innego użytkownika do grupy, sprawia że nowy użytkownik automatycznie odziedziczy wszystkie zasady i uprawnienia już przypisane do tej grupy
- Może ułatwić zarządzanie uprawnieniami dla wielu użytkowników



Polityka uprawień (Policy)

- Obiekt w AWS, który po skojarzeniu z zasobem definiuje jego uprawnienia
- Przechowywana w AWS jako dokument JSON
- Uprawnienia określają, kto ma dostęp do zasobów i jakie akcje może wykonywać

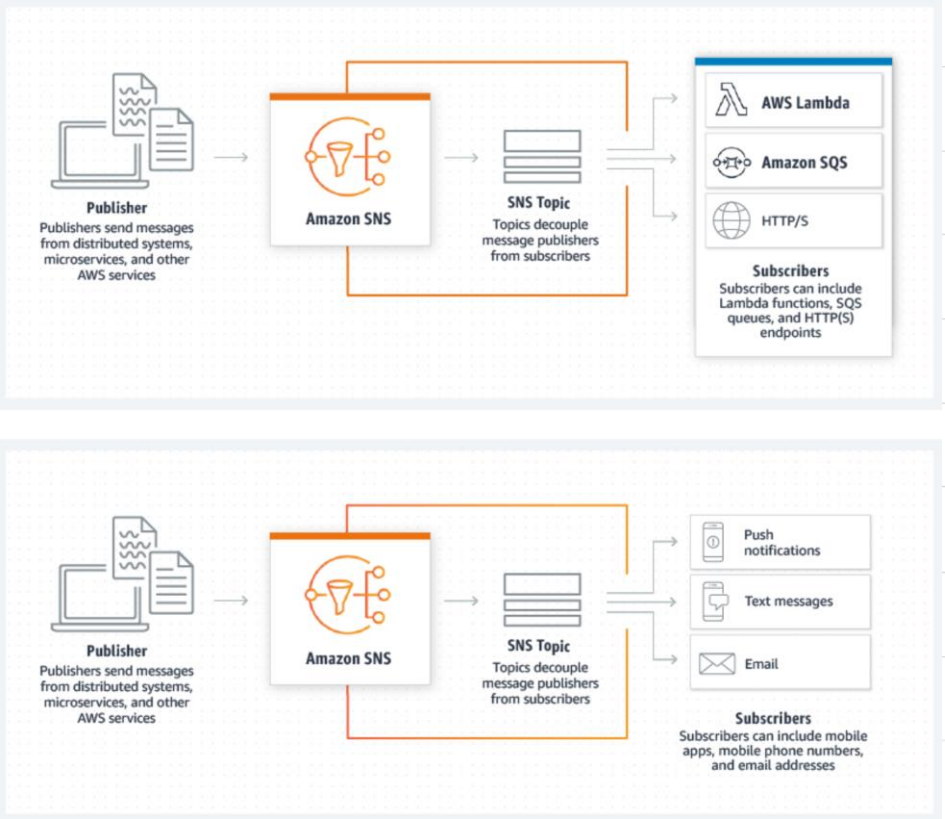


Konto roota

- Każde nowo stworzone konto AWS, zaczynasz od tożsamości jednokrotnego logowania, która ma pełny dostęp do wszystkich usług i zasobów AWS na koncie

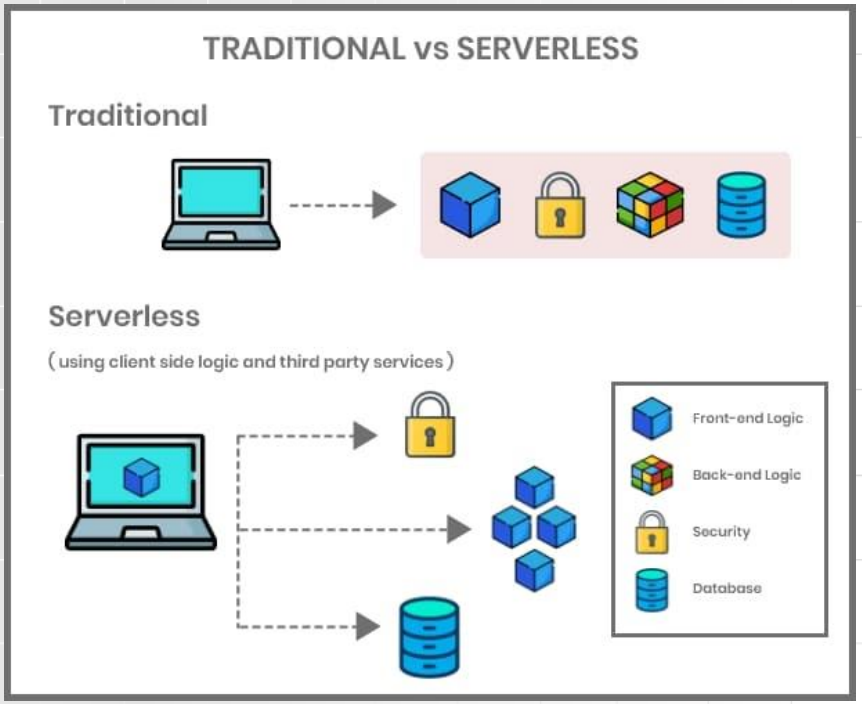
AWS SNS

- Tworzenie Tematów
- Zarządzanie Subskrypcjami
- Filtrowanie Wiadomości
- Różne Typy Subskrypcji - HTTP/S, E-mail, SMS, AWS SQS
- Skalowalność i Elastyczność
- Proste i Elastyczne Integracje
- Bezpieczeństwo
- Wsparcie dla Wiadomości Strukturalnych
- Wieloplatformowość



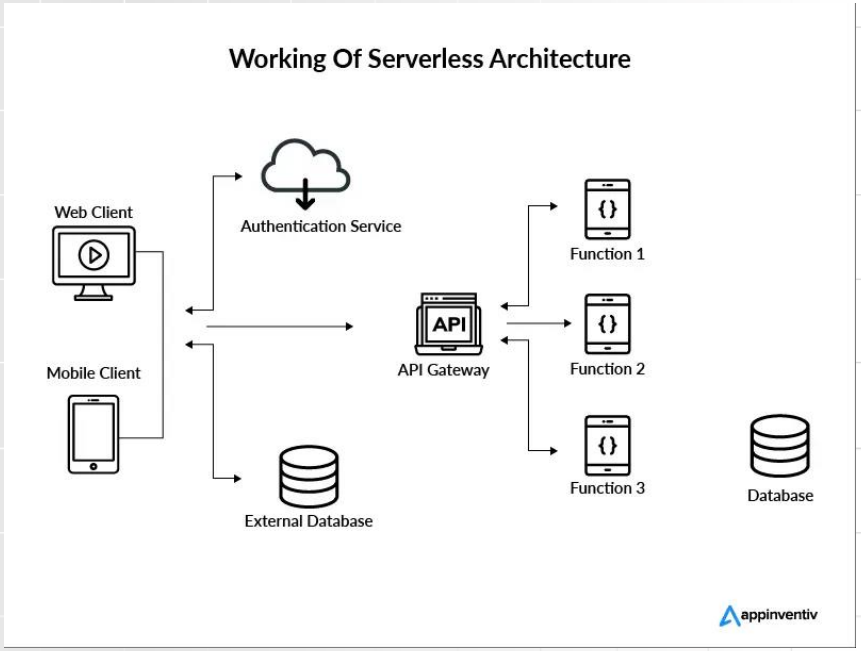
Architektura serverless

- Sposób na tworzenie i uruchamianie aplikacji i usług bez konieczności zarządzania infrastrukturą
- Aplikacja nadal działa na serwerach, ale całe zarządzanie serwerem jest wykonywane przez AWS
- Nie ma konieczności udostępniać, skalować i utrzymywać serwerów, aby uruchamiać aplikacje, bazy danych i systemy pamięci masowej



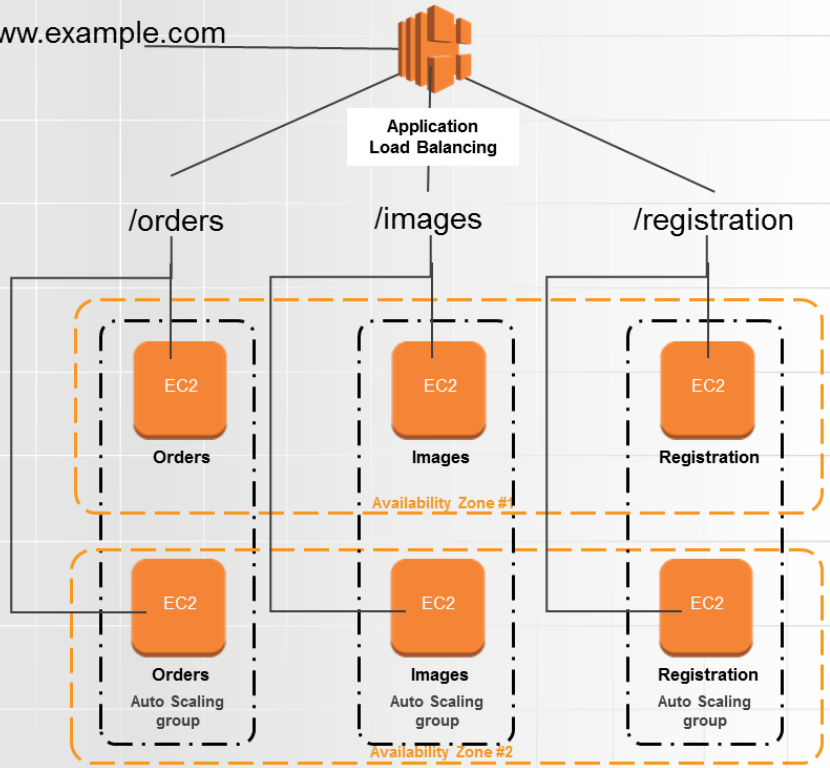
Lambda [1]

- Pozwala uruchamiać kod bez udostępniania lub zarządzania serwerami
- Płatność tylko za zużyty czas obliczeniowy — nie ma opłat, gdy Twój kod nie jest uruchomiony
- Płatność dopiero po pierwszym milionie żądań miesięcznie na AWS Free Tier
- Dzięki Lambdzie można uruchamiać kod dla praktycznie każdego typu aplikacji lub usługi (wszystko to bez konieczności administrowania).



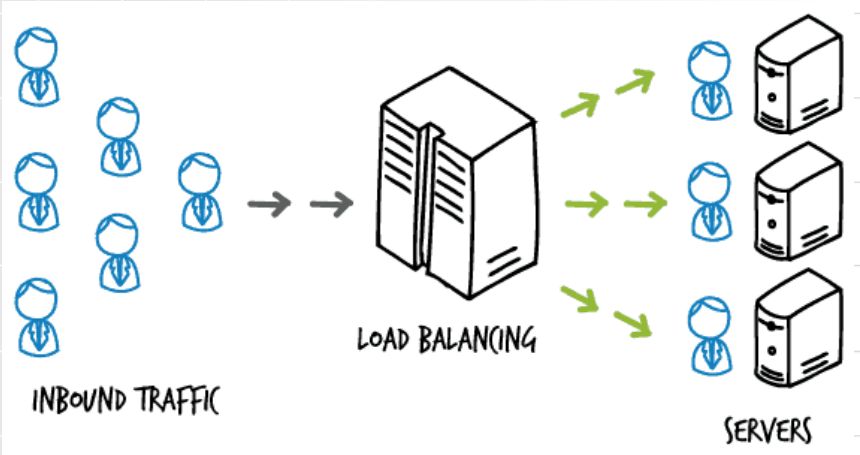
Application Load Balancer [1]

- Najlepiej nadaje się do równoważenia obciążenia ruchem Hypertext Transfer Protocol (HTTP) i Secure HTTP (HTTPS)
- Zapewnia zaawansowane kierowanie żądań ukierunkowane na dostarczanie nowoczesnych architektur aplikacji, w tym mikrousług i kontenerów
- Działa na poziomie indywidualnego żądania (warstwa 7)



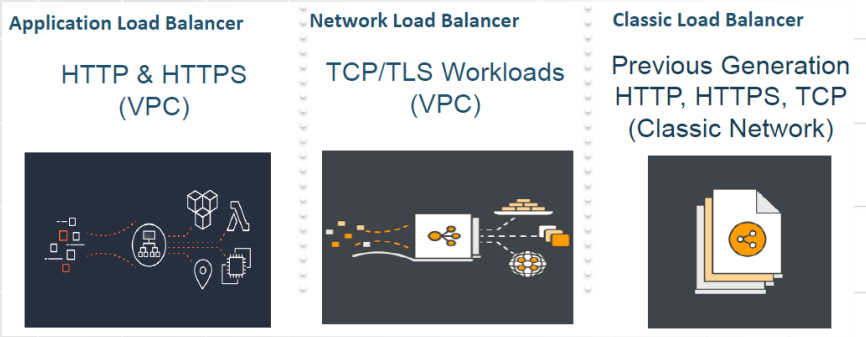
Network Load Balancer [1]

- Najlepiej nadaje się do równoważenia obciążenia ruchu protokołu kontroli transmisji (TCP), protokołu datagramów użytkownika (UDP) i protokołu TLS (Transmission Layer Security), gdzie wymagana jest ekstremalna wydajność.
- Działa na poziomie połączenia (warstwa 4),
- Kieruje ruch do celów w Amazon VPC i jest w stanie obsłużyć miliony żądań na sekundę przy zachowaniu bardzo niskich opóźnień.



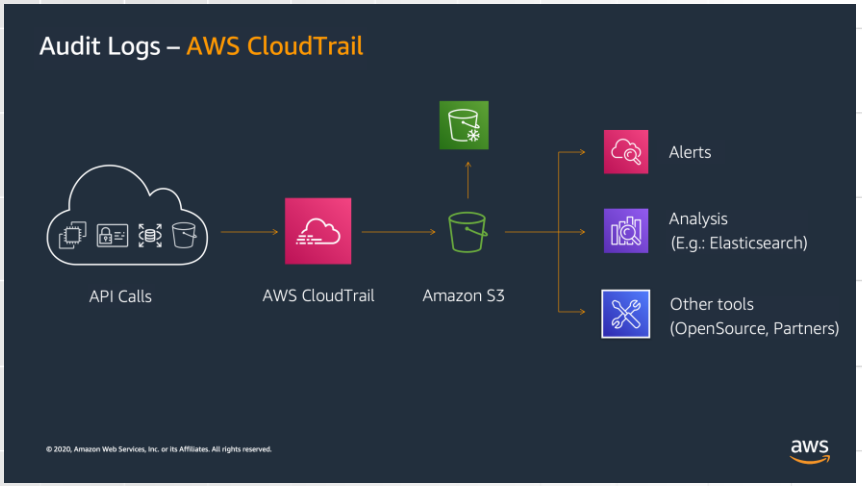
Classic Load Balancer [1]

- Zapewnia podstawowe równoważenie obciążenia w wielu instancjach EC2 i działa na poziomie żądania i połączenia.
- Działa na poziomie połączenia (warstwa 4) oraz na poziomie indywidualnego żądania (warstwa 7),
- AWS odradza korzystania z Classic Load Balancer na korzyść ALB I NLB
- Istnieje bardzo niewiele scenariuszy, w których preferowane byłoby użycie ELB



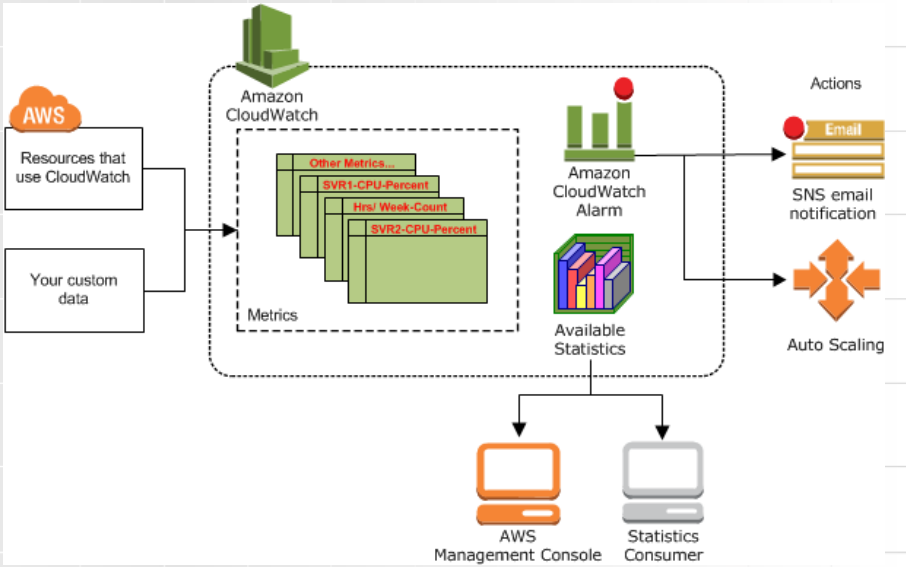
CloudTrail

- Umożliwia zarządzanie, zgodność, audyty operacyjne i audyty ryzyka konta AWS.
- Monitoruje każdą akcję wykonywaną na koncie AWS w celach bezpieczeństwa
- Jest to bardzo przydatne ze względów bezpieczeństwa, aby administratorzy mogli wiedzieć, kto używa ich konta i co robią.
- Jeśli coś pójdzie nie tak lub pojawi się problem z bezpieczeństwem, CloudTrail będzie najlepszym dowodem, aby dowiedzieć się, co się stało



CloudWatch [1]

- CloudWatch to usługa monitorowania do monitorowania zasobów AWS i aplikacji, które uruchamiasz na AWS
- CloudWatch monitoruje, co robią różne usługi i jakie zasoby wykorzystują.
- Jeśli CloudTrail jest monitorem ludzi, CloudWatch jest monitorem usług
- Pozwala używać metryk do obliczania statystyk, a następnie prezentować dane graficznie
- Pozwala tworzyć własne metryki

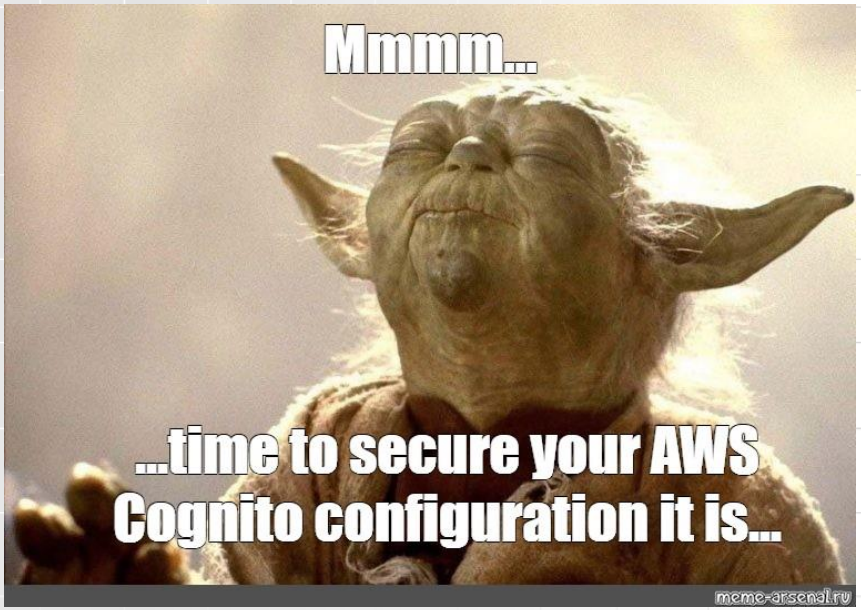


AWS Config

- Umożliwia audyt i ocenę konfiguracji Twoich zasobów AWS
- AWS Config stale monitoruje i rejestruje konfiguracje zasobów AWS i pozwala zautomatyzować ocenę zarejestrowanych konfiguracji względem pożądanych konfiguracji
- Przykładem może być reguła nie pozwalająca otwarcia portu 22, jeżeli taki port zostanie otwarty to zostaniemy o tym poinformowani

AWS Cognito [1]

- Usługa **zarządzania tożsamościami i dostępem do danych użytkowników**
- Zapewnia **rozwiązania** dla **aplikacji webowych** i **mobilnych**, umożliwiając bezpieczne dodawanie **funkcji logowania**, **rejestracji** oraz **zarządzania tożsamościami** użytkowników.
- **Umożliwia dostosowywanie procesów logowania i rejestracji**, w tym dodawanie własnych walidacji i logiki.
- Pozwala na **autentykację użytkowników poprzez zewnętrznych dostawców tożsamości**, takich jak Google, Facebook, Amazon oraz przez dostawców korzystających z protokołów OpenID Connect i SAML.
- Obsługuje **logowanie za pomocą nazwy użytkownika i hasła**, **logowanie przez zewnętrznych dostawców tożsamości** oraz inne opcje.



Wrocław
University
of Science
and Technology

Dziękuję za uwagę