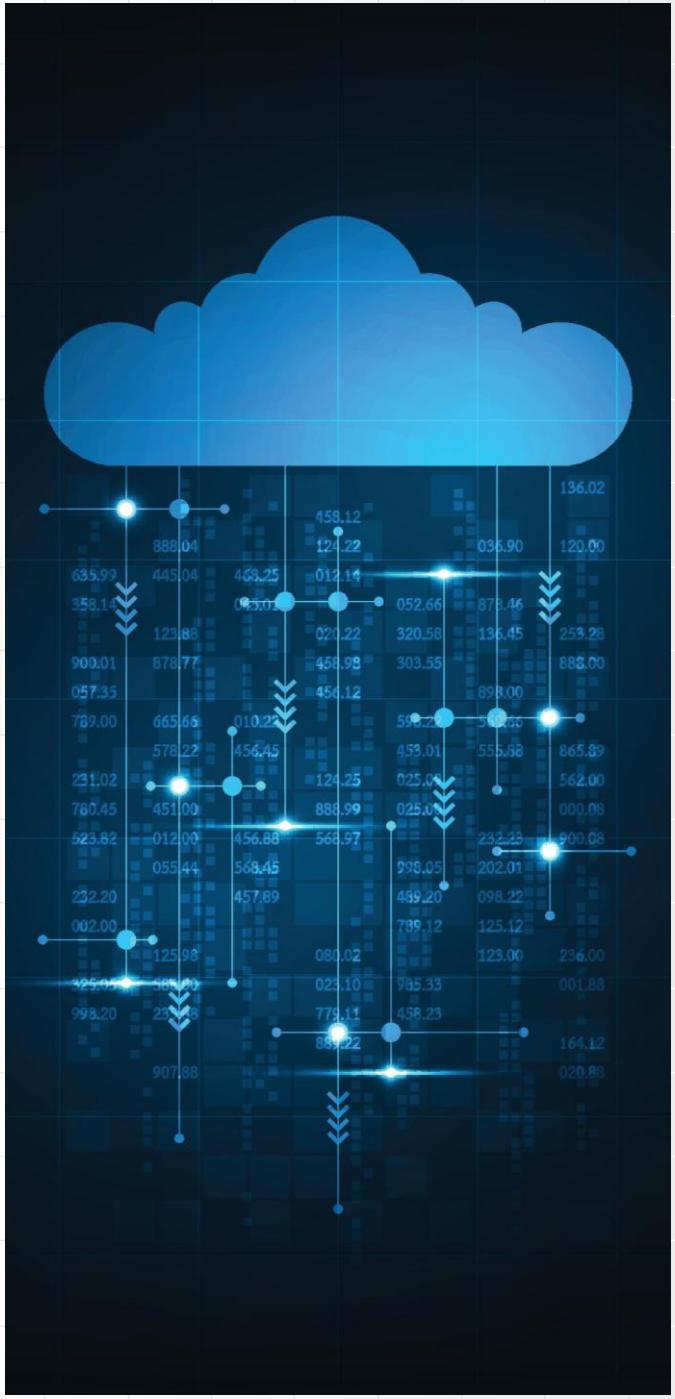


Programowanie w chmurze

Rafał Palak

Politechnika Wrocławska

AWS S3

- nazwę S3, która jest „jednym z popularnych narzędzi open-source”.
- Prawie 100 milionów nieautoryzowanych prób tworzenia nowych plików w S3 (żądania PUT) w ciągu jednego dnia.
- Rachunek wyniósł ponad 1 300 USD.
- "All this actually happened just a few days after I ensured my client that the price for AWS services will be negligible, like $20 at most for the entire month," https://medium.com/@maciej.pocwierz/how-an-empty-s3-bucket-can-make-your-aws-bill-explode-934a383cb8b1

AWS S3

S3 Object Lambda pricing example

You have 1,000,000 objects that contain historical log data, generated by many applications. Confidential log entries make up 50% of the data. These logs are stored in the S3 Standard storage class, and the average object size is 1000 KB. You are building an application that analyzes this data, but should not have access to confidential log entries.

You can use S3 Object Lambda to filter out confidential log entries. This filtering occurs as your logs are retrieved from S3 with standard S3 GET requests. The Lambda function to filter your data is allocated 512MB of memory, has a 1 second runtime, and returns filtered objects that are 500 KB in size (on average) back to your application. This example assumes one retrieval per month for each object. This example uses the US East (N. Virginia) Region.

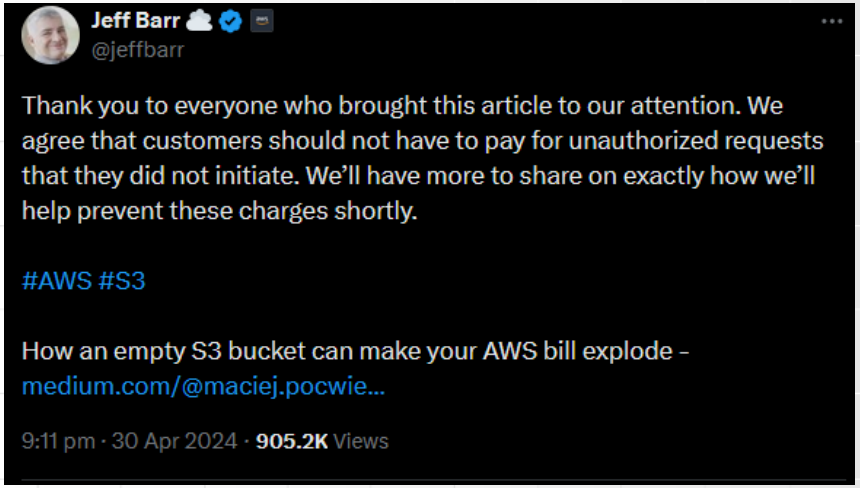
Your charges would be calculated as follows:

Amazon S3 GET request charge

S3 GET requests from the S3 Standard storage class cost $0.0004 per 1,000 requests.

S3 GET Request cost: 1,000,000 requests * $0.0004/1K requests = **$0.40**

https://aws.amazon.com/s3/pricing/



AWS S3 – wnioski*

- Każdy, kto zna nazwę któregokolwiek z Twoich zasobników S3, może zwiększyć rachunek za AWS według własnego uznania.
- Dodanie losowego przyrostka do nazw zasobników może zwiększyć bezpieczeństwo.
- Podczas wykonywania wielu żądań do S3 upewnij się, że wyraźnie określasz region AWS.

*wnioski wyciągnięte w cytowanym artykule https://medium.com/@maciej.pocwierz/how-an-empty-s3-bucket-can-make-your-aws-bill-explode-934a383cb8b1

AWS S3 -zmiany

Posted on: Aug 19, 2024

Amazon S3 has completed a change so unauthorized requests that customers did not initiate are free of charge. With this change, bucket owners will never incur request or bandwidth charges for requests that return an HTTP 403 (Access Denied) error response if initiated from outside their individual AWS account or AWS Organization. To see the full list of error codes that are free of charge, visit Billing for Amazon S3 error responses. This billing change requires no changes to customer applications and applies to all S3 buckets.

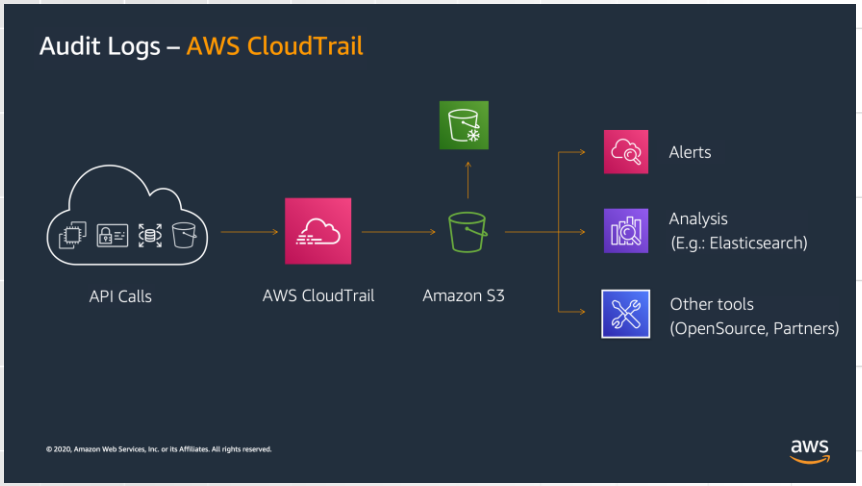
https://aws.amazon.com/about-aws/whats-new/2024/08/amazon-s3-no-charges-several-http-error-codes/?utm_source=chatgpt.com

Wrocław
University
of Science
and Technology

Monitoring

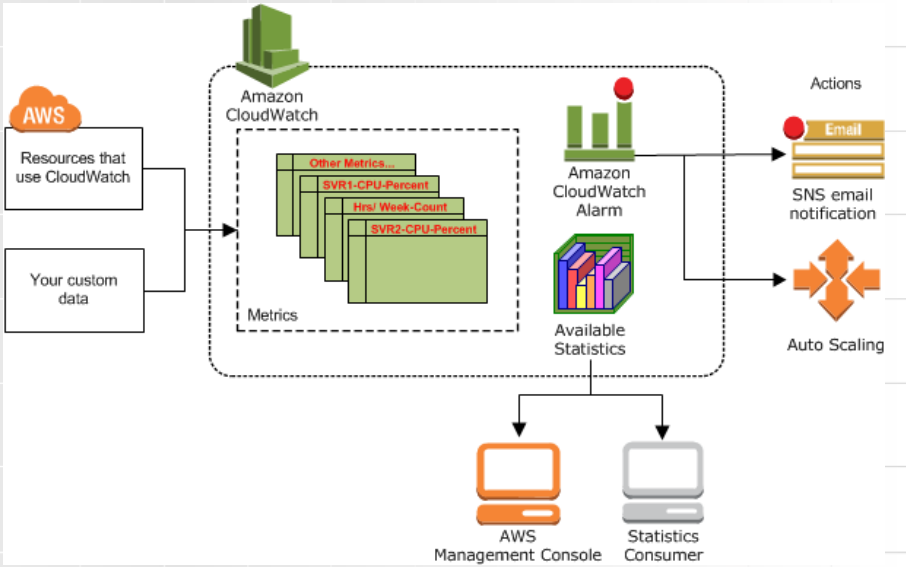
CloudTrail

- 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



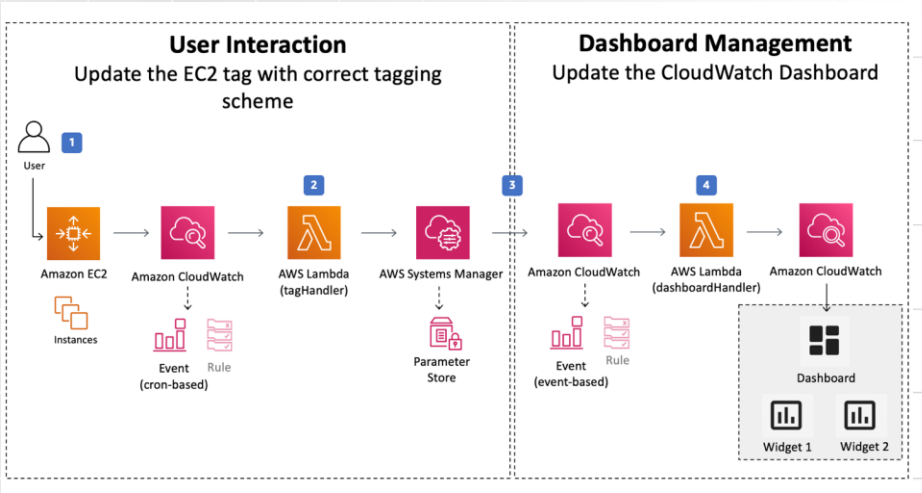
CloudWatch [1]

- 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

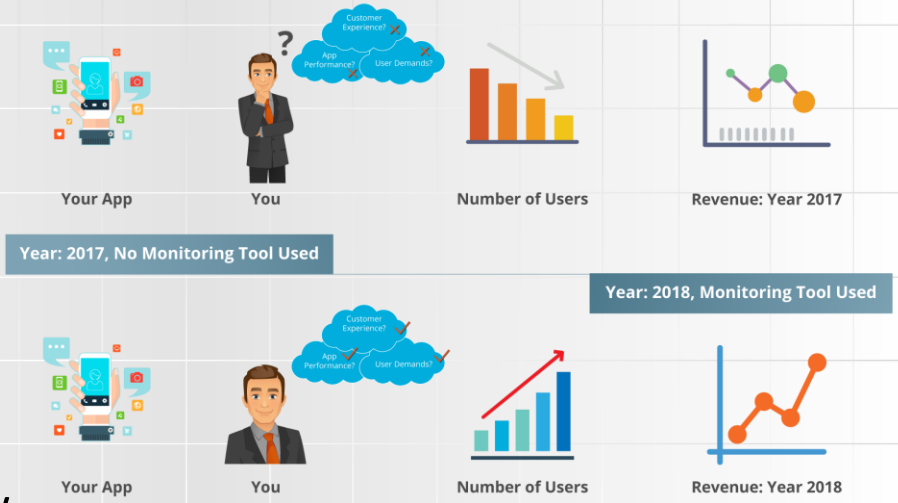


CloudWatch [2]

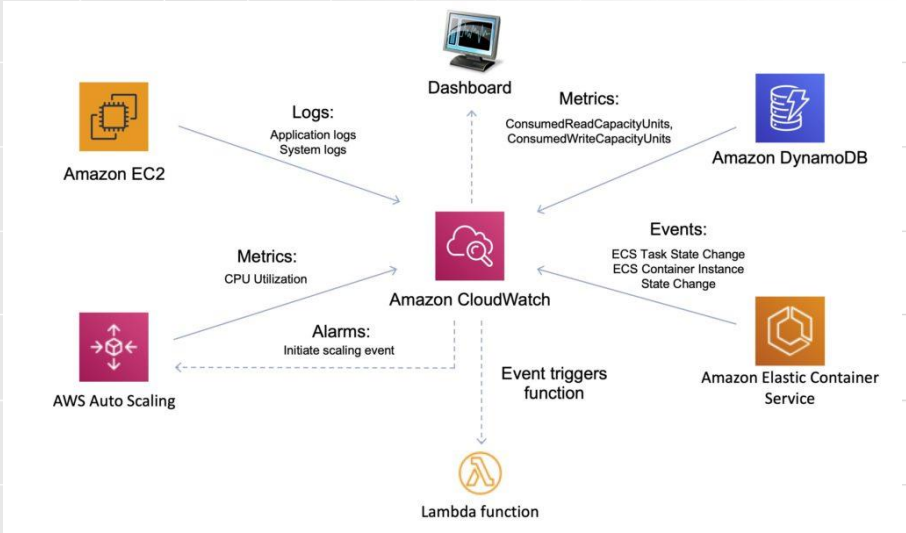
- Pozwala monitorować w czasie rzeczywistym zasoby i aplikacje korzystających z AWS
- Pozwala skonfigurować akcje alarmowe, aby zatrzymać, uruchomić lub kończyć działanie instancji Amazon EC2 po spełnieniu określonych kryteriów
- Pozwala tworzyć alarmy, które inicjują działania automatycznego skalowania Amazon EC2 i Amazon Simple Notification Service (Amazon SNS) bez konieczności ingerencji użytkownika



CloudWatch [3]

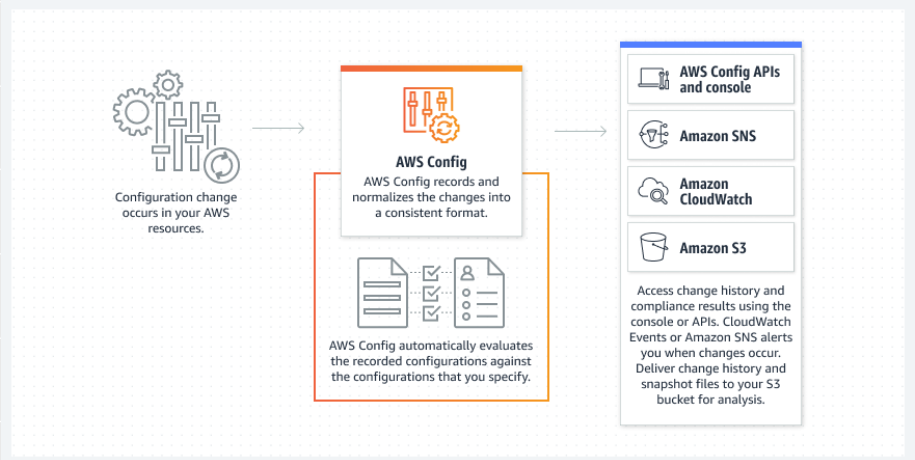


- CloudWatch doskonale nadaje się do upewniania się, że usługi w chmurze działają płynnie i nie zużywają więcej lub mniej zasobów, niż powinny
- CloudWatch pozwala upewnić się że wszystkie zasoby są uruchomione, co może być trudne, jeśli duża firma używa setek różnych maszyn i dysków. Monitory i alarmy można skonfigurować za pomocą CloudWatch, aby automatycznie inicjował alert, gdy metryka osiągnie określony limit.



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

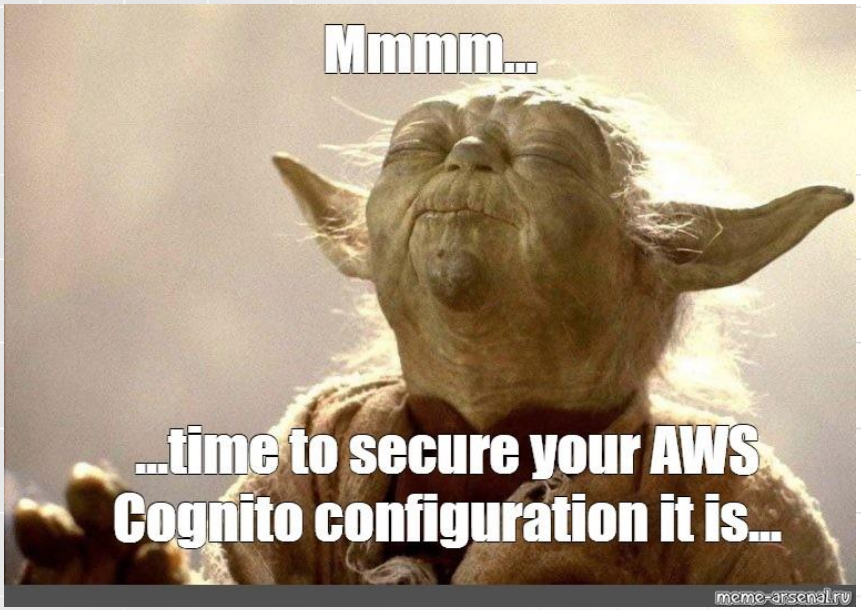


Wrocław
University
of Science
and Technology

AWS Cognito

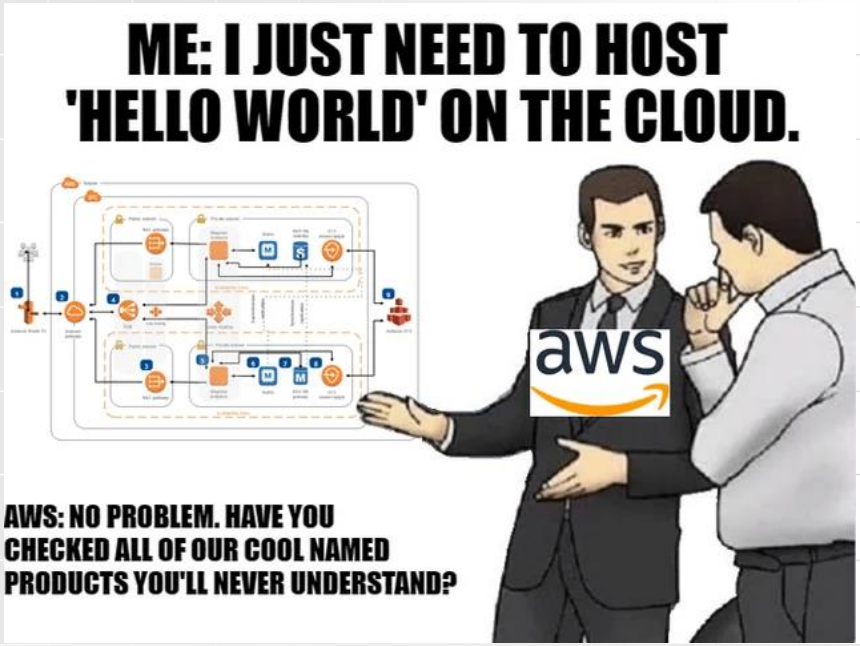
AWS Cognito [1]

- 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.



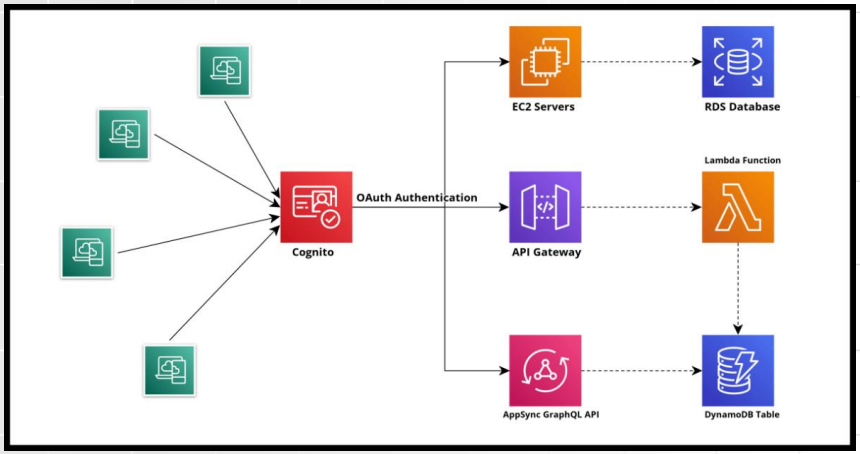
AWS Cognito [2]

- **Wspiera MFA** (Wieloskładnikowe uwierzytelnianie), co zwiększa bezpieczeństwo poprzez wymaganie dodatkowej formy weryfikacji użytkownika podczas logowania.
- Jest zaprojektowane tak, aby **łatwo skalować się w miarę rosnącej liczby użytkowników** aplikacji, co jest istotne dla rosnących firm i aplikacji.
- Oferuje **bogaty zestaw SDK i API**, które ułatwiają integrację z różnymi platformami programistycznymi i aplikacjami.



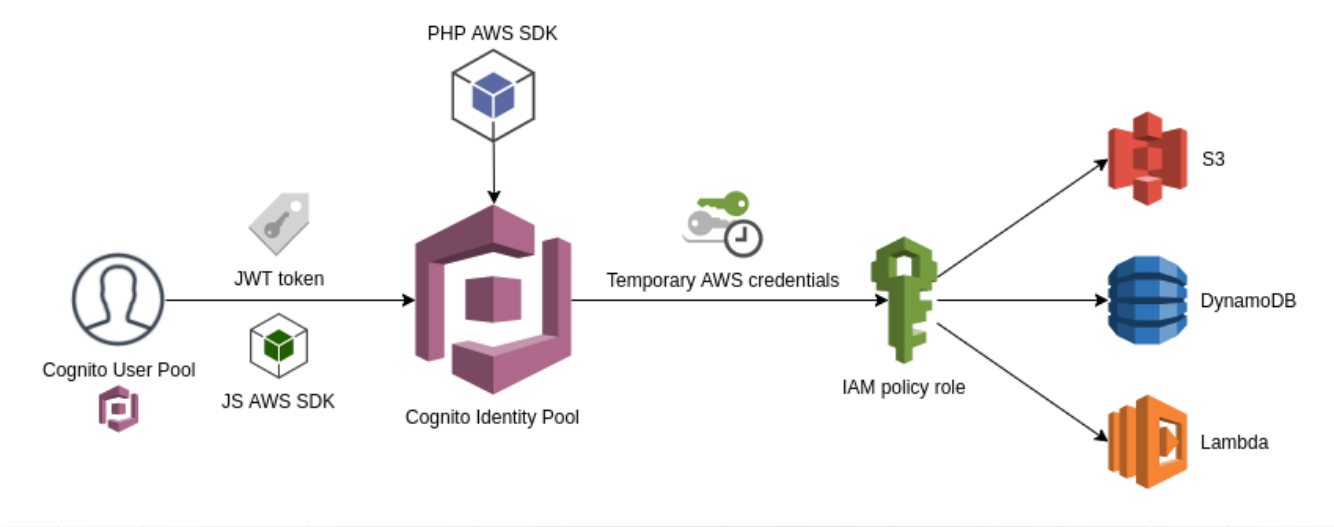
AWS Cognito – dlaczego?

- **Uproszczenie procesu tworzenia, zarządzania i personalizacji profili użytkowników** z automatycznymi funkcjami zarządzania cyklem życia użytkownika.
- **Elastyczne i skalowalne rozwiązania uwierzytelniające**, które mogą obsługiwać od kilku do milionów użytkowników bez konieczności ręcznego zwiększania zasobów.
- **Wsparcie dla wielu dostawców tożsamości** przy **minimalnym nakładzie** kodowania i konfiguracji.
- Oferuje wysokie bezpieczeństwo danych użytownika poprzez **szyfrowanie danych w spoczynku** i **w tranzycie**, **opcje wieloskładnikowego uwierzytelniania** (MFA), i zgodność z międzynarodowymi standardami bezpieczeństwa.



AWS Cognito – dlaczego?

- Pomaga w **utrzymaniu zgodności z przepisami dotyczącymi danych**, dzięki wbudowanym funkcjom bezpieczeństwa i prywatności.
- Umożliwia **tworzenie zaawansowanych profili użytkowników**, które umożliwiają personalizację i lepszą interakcję z aplikacją.

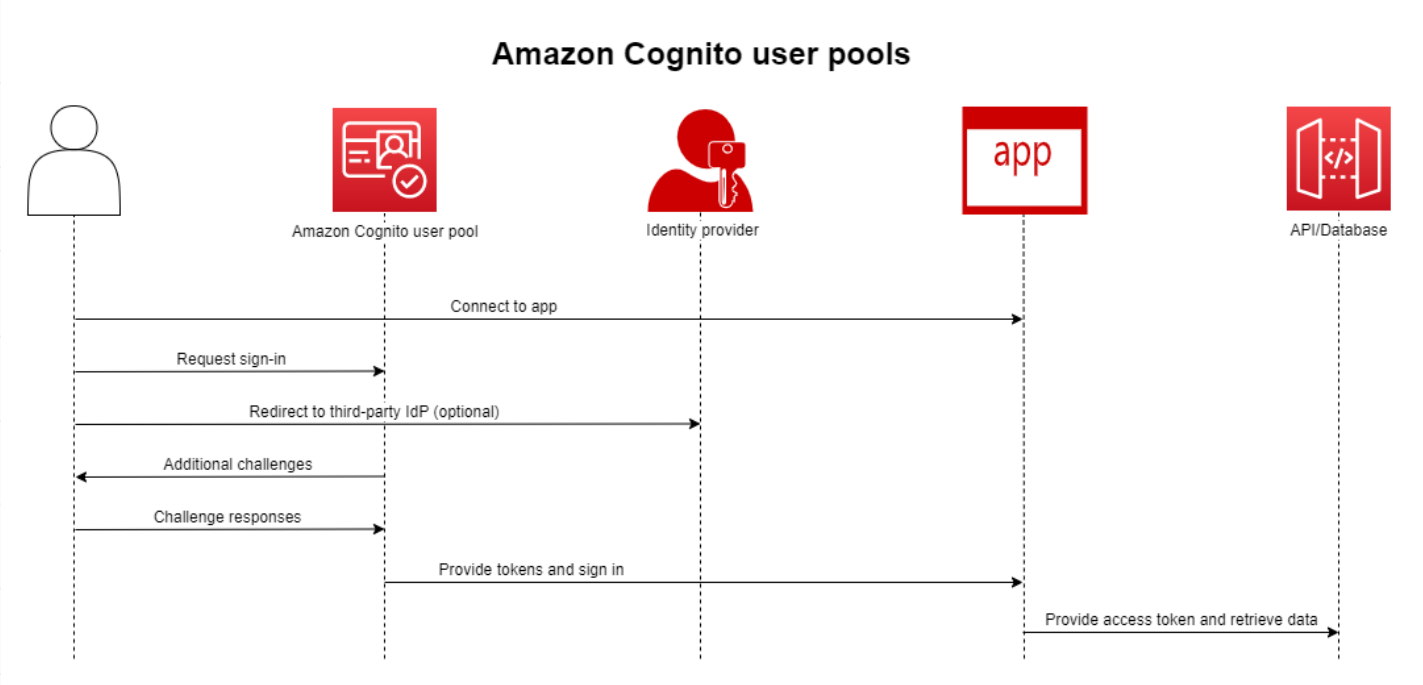


Wrocław
University
of Science
and Technology

AWS Cognito - Główne komponenty

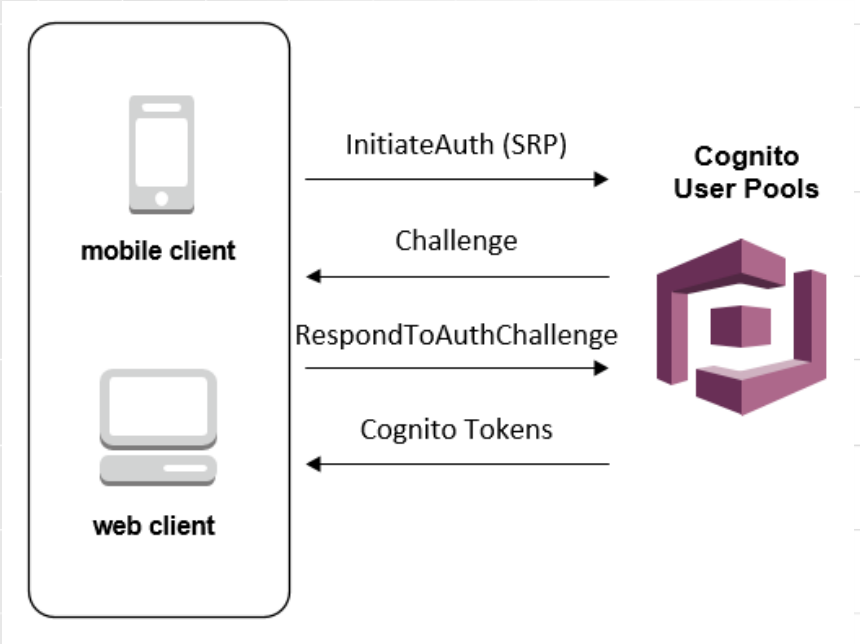
User Pools

- Jedna z **dwóch głównych funkcji oferowanych przez AWS Cognito**, służąca do zarządzania katalogiem użytkowników i obsługi ich uwierzytelniania w aplikacjach mobilnych i internetowych.



User Pools - główne cechy i funkcje

- Umożliwiają **tworzenie własnych katalogów użytkowników**.
- Umożliwiają **rejestrację**, **logowanie** i **zarządzanie profilami** użytkowników.
- Obsługują **różne metody uwierzytelniania**, w tym z użyciem **nazwy użytkownika i hasła** oraz **uwierzytelnianie za pomocą mediów społecznościowych** (Facebook, Google, Amazon).
- Pozwala **definiować role** i **oparte na nich uprawnienia dostępu**, wykorzystując AWS IAM (Identity and Access Management) do zarządzania tym, jakie zasoby są dostępne dla poszczególnych użytkowników.

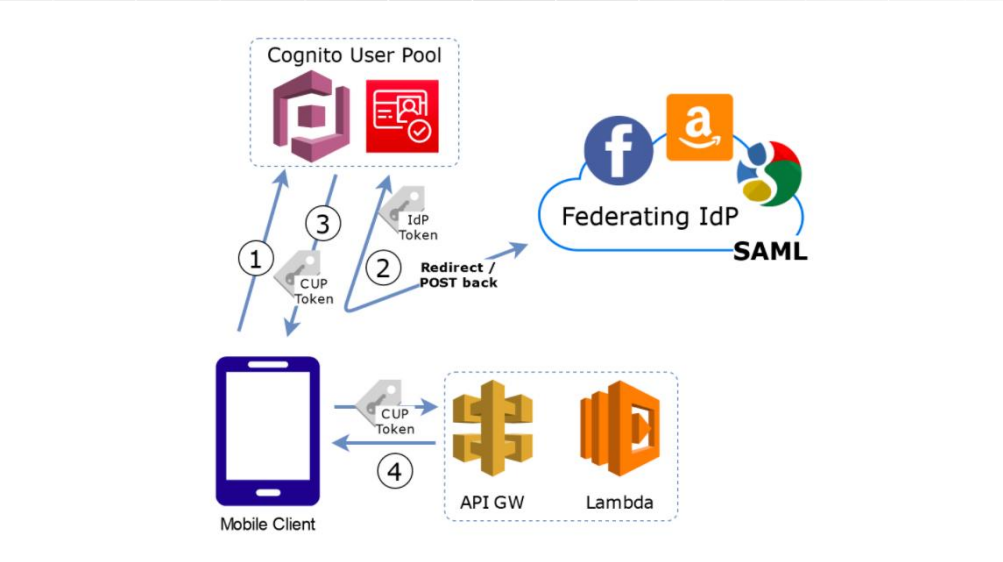


User Pools - zabezpieczenia

- Pozwala na **dodanie dodatkowej warstwy bezpieczeństwa** poprzez wymaganie drugiego czynnika uwierzytelnienia, np. SMS.
- Umożliwia określenie **wymagań dotyczących siły haseł**.
- **Pozwala na automatyczne blokowanie prób logowania** po przekroczeniu określonej liczby nieudanych prób.

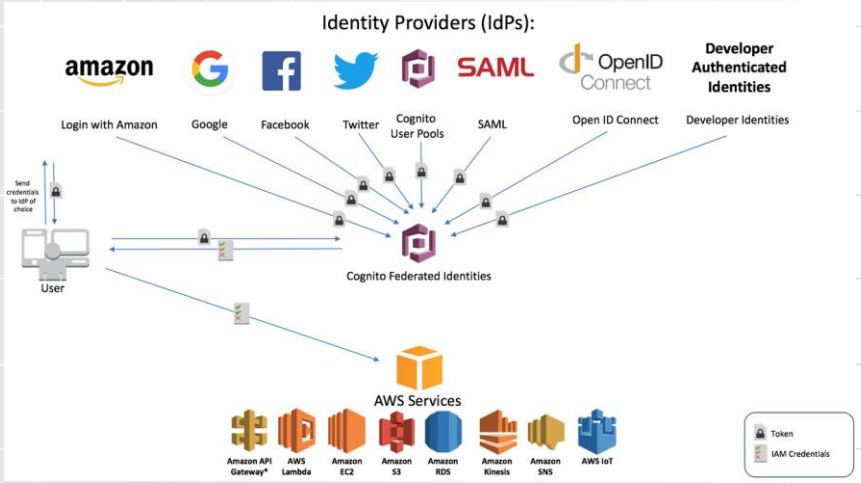
User Pools - personalizacja

- **Umożlwia personalizacje stron logowania** i **rejestracji**,
- User Pools można **integrować z AWS Lambda**, co pozwala na **uruchamianie niestandardowego kodu w odpowiedzi na różne zdarzenia** związane z cyklem życia użytkownika, np. przy rejestracji, potwierdzeniu użytkownika czy zmianie hasła.



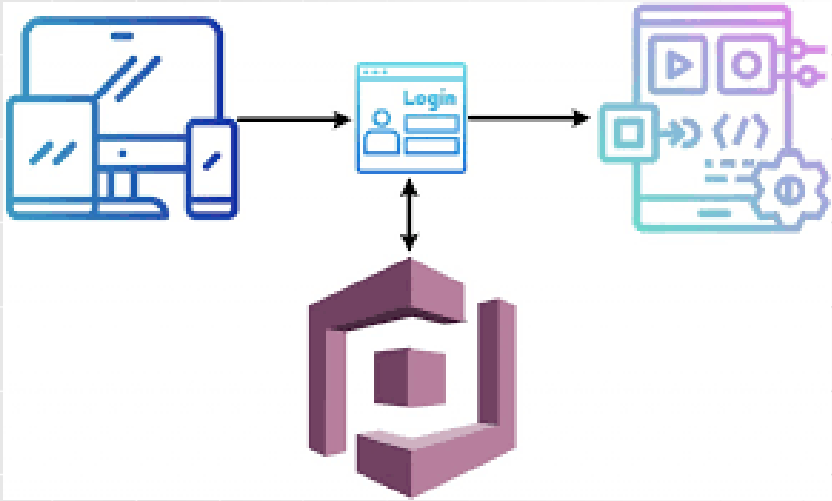
Identity Pools

- Znane również jako Federated Identity Pools
- Umożliwiają **zarządzanie tożsamościami użytkowników** i **udzielanie im dostępu do innych usług AWS**.
- Umożliwiają **integrację z różnymi dostawcami tożsamości** (np. Google, Facebook, Amazon, Apple) oraz **z własnymi systemami uwierzytelniania** poprzez SAML lub OpenID Connect.
- Wykorzystują **role IAM do nadawania uprawnień użytkownikom na podstawie ich tożsamości**. Użytkownicy otrzymują **tymczasowy dostęp do zasobów AWS** w oparciu o te role.
- **Możliwość implementacji własnych mechanizmów uwierzytelniania przez AWS** Lambda, co pozwala na tworzenie niestandardowych rozwiązań uwierzytelniających.



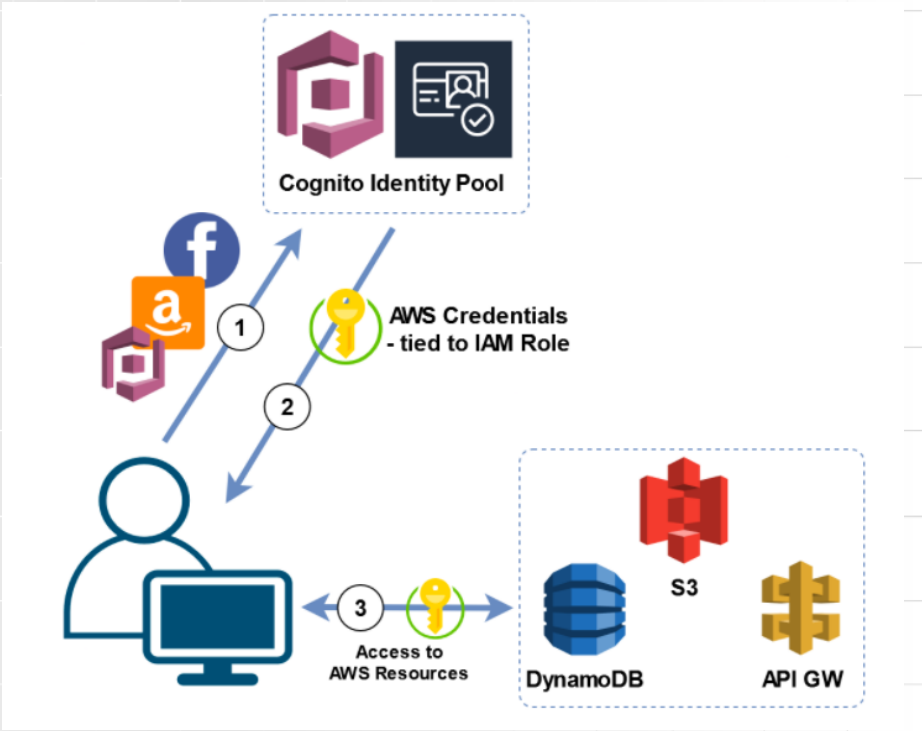
Identity Pools - zarządzanie dostępem

- **Role Based Access Control** (RBAC) - **Możliwość definiowania ról i zasad IAM**, które określają, **jakie operacje są dozwolone dla użytkowników autoryzowanych przez Identity Pool**.
- **Dynamiczne przypisywanie ról** - Możliwość stosowania **zasad**, które **dynamicznie przypisują role** na podstawie atrybutów sesji użytkownika, takich jak **identyfikator dostawcy tożsamości** czy **atrybuty użytkownika**.



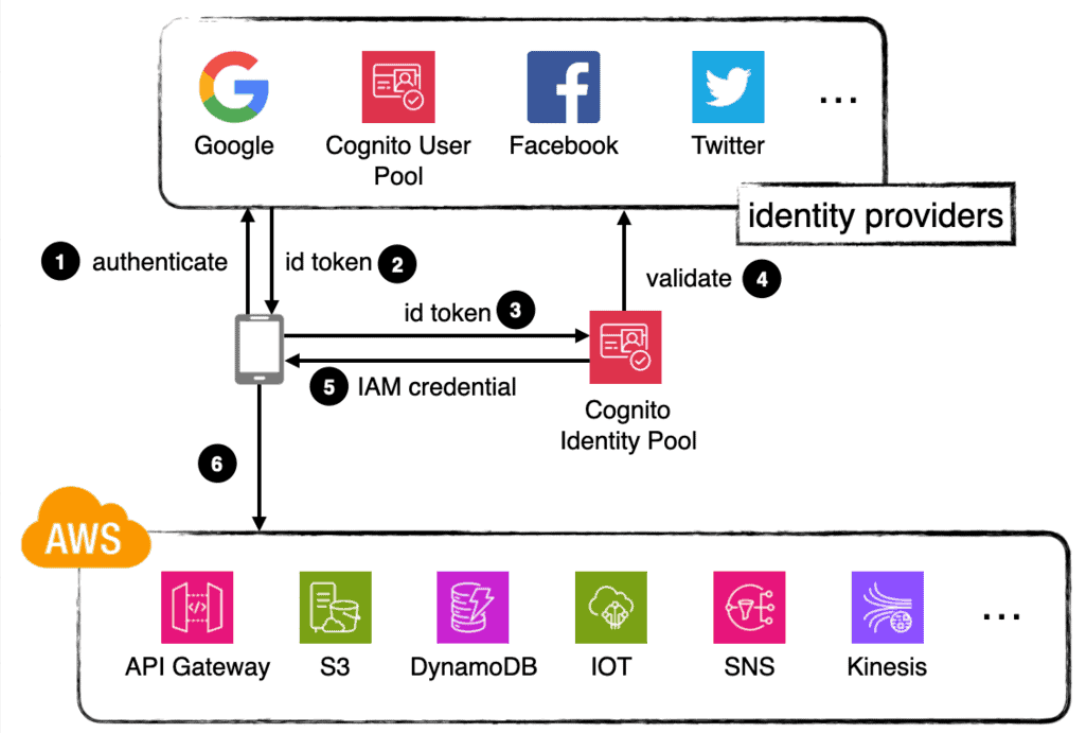
Identity Pools - zabezpieczenia

- Możliwość stosowania **warunkowych polityk bezpieczeństwa**, które mogą ograniczać dostęp na podstawie różnych czynników, jak lokalizacja użytkownika, urządzenie czy zachowania.
- Możliwość **włączenia wieloskładnikowego uwierzytelniania** dla dodatkowej warstwy bezpieczeństwa.



Identity Pools - zastosowanie

- Idealne **rozwiązanie dla aplikacji, które wymagają dostępu do zasobów AWS**, takich jak przechowywanie danych w S3 czy przetwarzanie w Lambda.
- Mogą być **używane do uwierzytelniania i autoryzacji urządzeń IoT**.



User Pools vs Identity Pools

- Służą jako **pełnoprawne rozwiązanie do zarządzania użytkownikami**. Pozwalają na **tworzenie i utrzymanie bazy użytkowników** dla **aplikacji internetowych** i **mobilnych**. Umożliwiają **rejestrację**, **logowanie** oraz **zarządzanie profilami** użytkowników.
- Skupiają się na **zarządzaniu użytkownikami i ich uwierzytelnianiu**

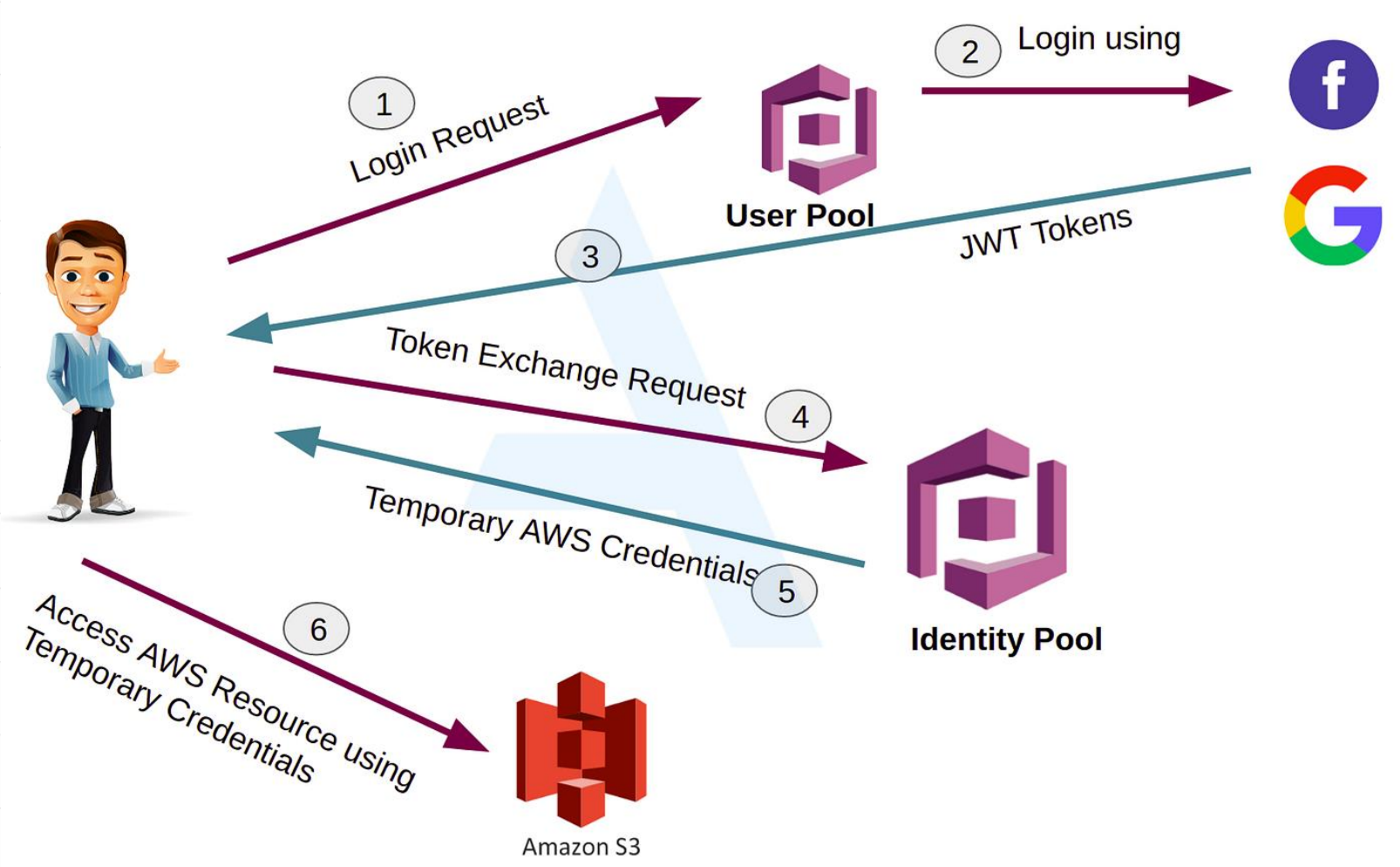
- Umożliwiają **zarządzanie tożsamościami** i **dostępem użytkowników do zasobów AWS**. Umożliwiają **integrację z różnymi źródłami** tożsamości, w tym z **User Pools**, aby przyznawać tymczasowe poświadczenia AWS do dostępu do zasobów.
- Koncentrują się na **autoryzacji dostępu do zasobów AWS**.
- Oferują **większą elastyczność** w **integracji z różnymi systemami tożsamości** niż User Pools.
- **Umożliwiają bardziej zaawansowane zarządzanie dostępem**, korzystając z ról IAM i polityk bezpieczeństwa.

User Pools vs Identity Pools

- Gdy istnieje potrzeba pełnej funkcjonalności zarządzania użytkownikami.
- Gdy aplikacja wymaga bezpośredniego uwierzytelniania użytkowników, bez konieczności dostępu do zasobów AWS.

- Gdy aplikacja wymaga dostępu do zasobów AWS.
- Gdy istnieje potrzeba pozwolenia użytkownikom logowania za pomocą różnych dostawców tożsamości.

Proces autoryzacji i uwierzytelniania

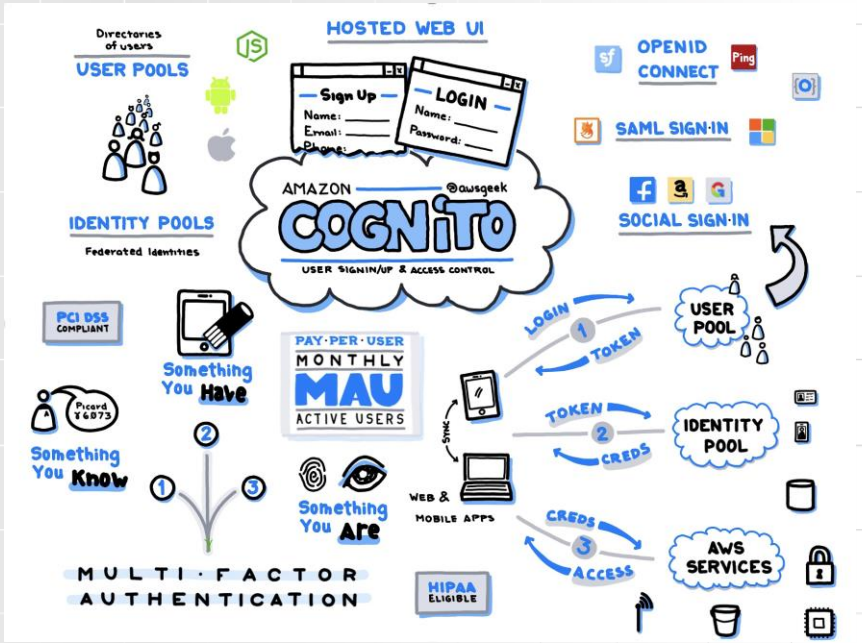


Wrocław
University
of Science
and Technology

AWS Cognito - Zabezpieczenia i zgodność

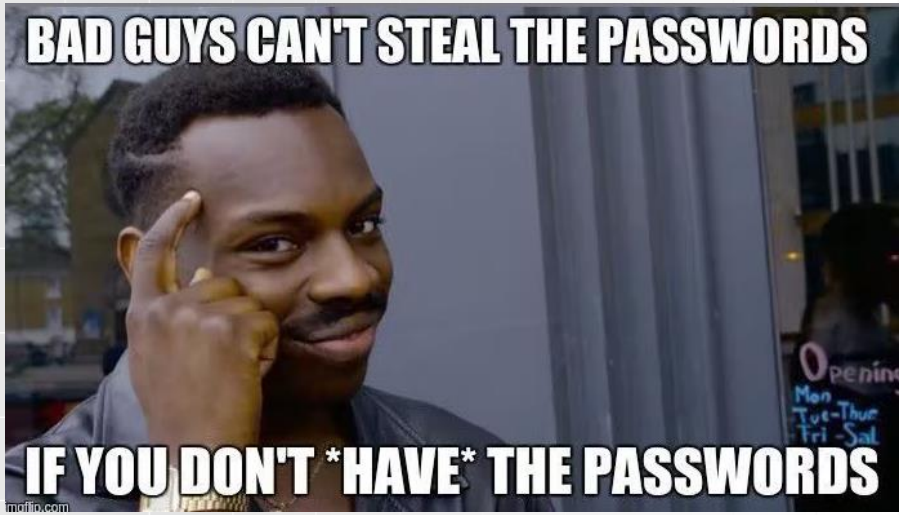
Funkcje bezpieczeństwa

- Pozwala na włączenie wieloskładnikowego uwierzytelniania, co znacząco zwiększa bezpieczeństwo poprzez wymaganie dodatkowej metody weryfikacji tożsamości użytkownika (np. SMS, telefon, aplikacja uwierzytelniająca).
- Zapewnia automatyczne szyfrowanie danych przechowywanych, jak i transmisji przy użyciu protokołu HTTPS. Możliwe jest również użycie własnych kluczy szyfrujących zarządzanych przez AWS Key Management Service (KMS) dla dodatkowej kontroli.



Funkcje bezpieczeństwa

- Pozwala określić **polityki bezpieczeństwa** dla użytkowników, takie jak **zasady dotyczące skomplikowania hasła**, **czasu jego ważności** i **blokady konta po określonej liczbie nieudanych** prób logowania.
- Integruje się z **AWS CloudTrail**, co **umożliwia rejestrowanie i monitorowanie wszystkich zapytań do usługi Cognito API**, zapewniając możliwość przeprowadzania szczegółowych audytów bezpieczeństwa.



Wrocław
University
of Science
and Technology

Dziękuję za uwagę