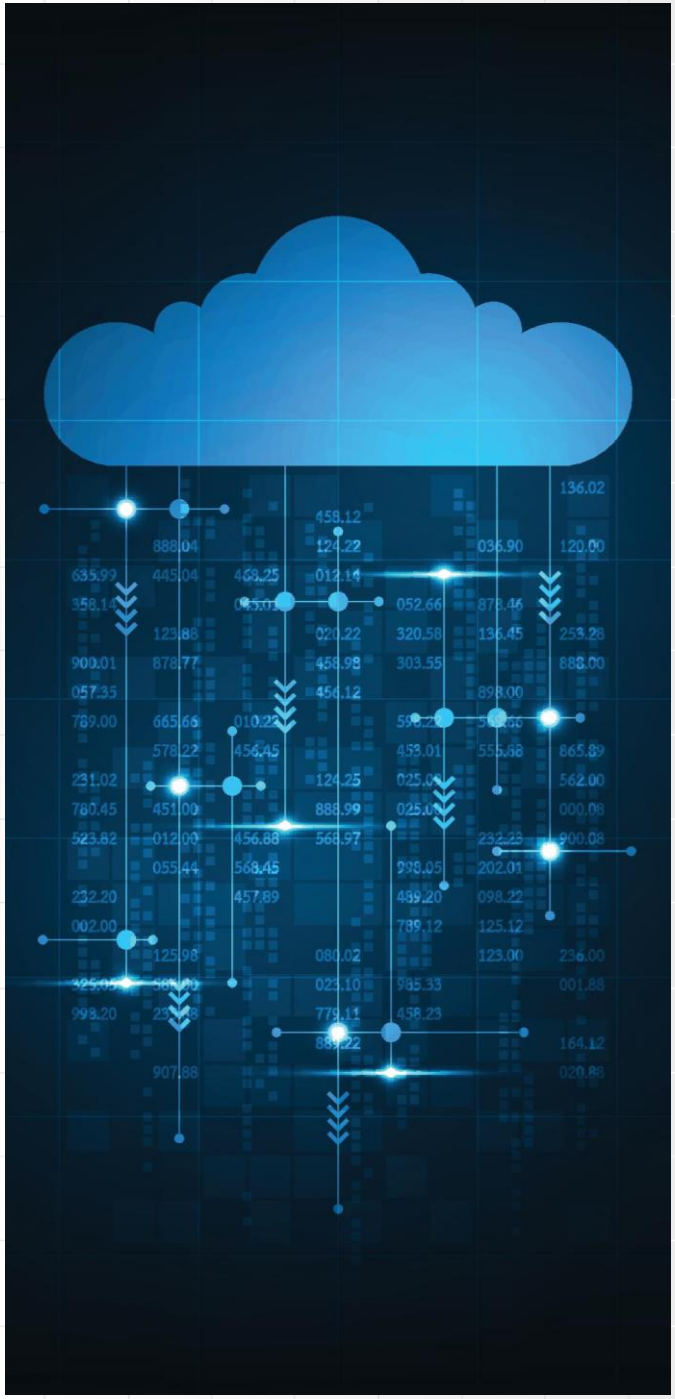


Programowanie w chmurze

Rafał Palak

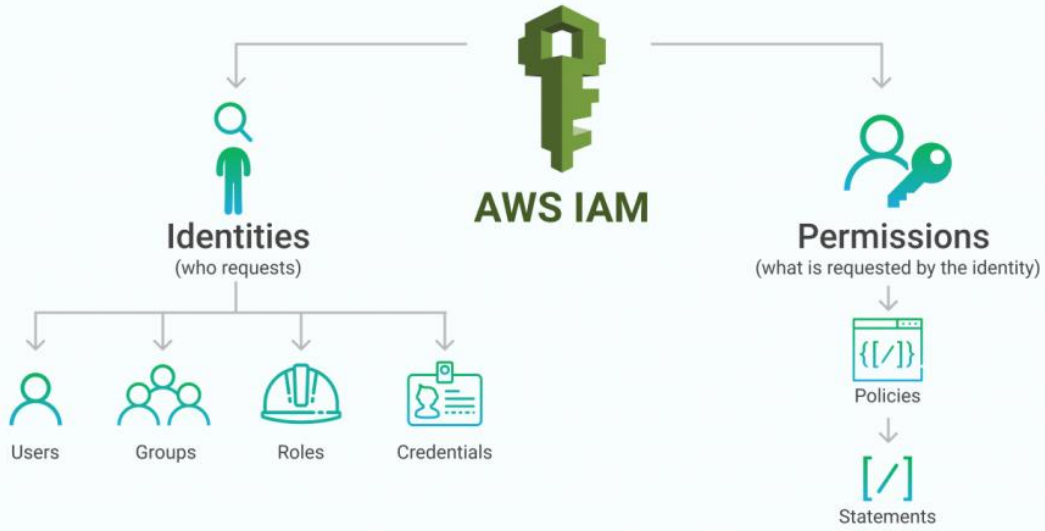
Politechnika Wrocławska

Wrocław
University
of Science
and Technology

Identity and Access Management

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



AWS Identity and Access Management (IAM) [2]

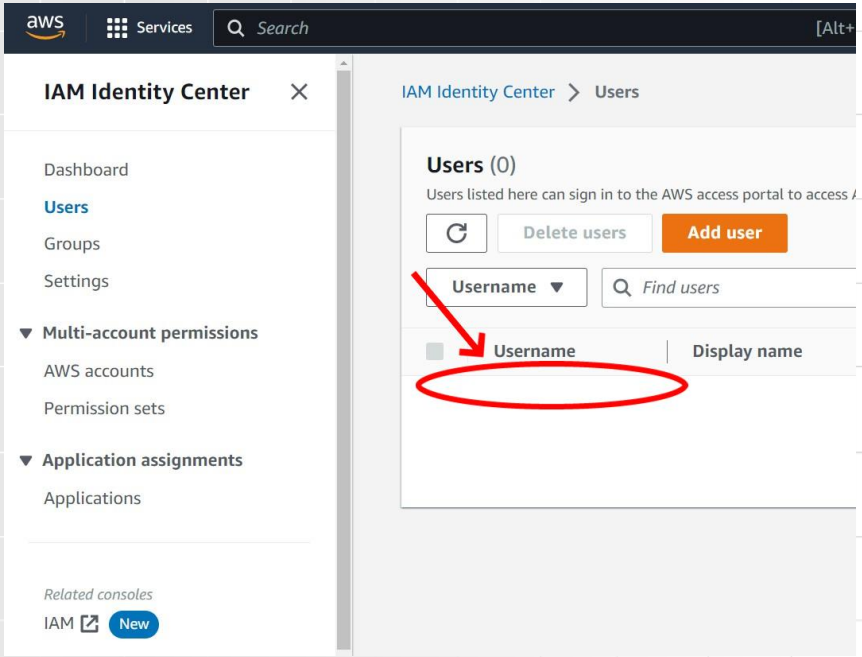
- Kluczowy element zabezpieczeń w chmurze, który zapewnia kontrolę nad kto i w jaki sposób może korzystać z zasobów AWS, a także jakie operacje mogą być na nich wykonywane.
- W dużych organizacjach, gdzie wielu użytkowników wymaga dostępu do zasobów AWS, trudno jest śledzić, kto ma dostęp do czego.
- Konieczność zapewnienia, że użytkownicy mają tylko te uprawnienia, które są im niezbędne do wykonania ich pracy, bez narażania zasobów na nieuprawniony dostęp.

AWS Identity and Access Management (IAM) [3]

- Skoncentrowany na zarządzaniu tożsamościami i uprawnieniami
- Zapewnia zaawansowane mechanizmy autentykacji, w tym uwierzytelnianie wieloskładnikowe (MFA), co znacząco zwiększa bezpieczeństwo dostępu do zasobów.
- Umożliwia federację tożsamości, co pozwala użytkownikom na logowanie się do usług AWS przy użyciu ich istniejących poświadczeń organizacyjnych (np. Active Directory.
- Zapewnia szczegółowe logi i historię działań użytkowników, umożliwiając audyt, monitorowanie i analizę działań związanych z dostępem do zasobów AWS.

AWS IAM Identity Center [1]

- Jest usługą umożliwiającą zarządzanie jednolitym dostępem i tożsamościami użytkowników do wielu kont i aplikacji, zarówno w AWS, jak i poza nim.
- Skupia się na upraszczaniu zarządzania dostępem do wielu kont AWS oraz aplikacji SaaS i wewnętrznych.
- Obejmuje Single Sign-On (SSO), co umożliwia użytkownikom logowanie się do wielu kont AWS i aplikacji za pomocą pojedynczych poświadczeń.

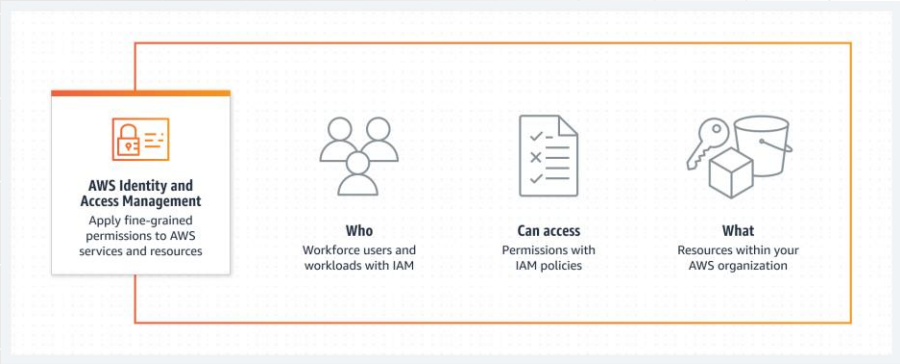


AWS IAM Identity Center [2]

- Umożliwia integrację z zewnętrznymi dostawcami tożsamości (IdP), takimi jak Microsoft Active Directory, co pozwala na centralne zarządzanie tożsamościami.
- Umożliwia prostsze zarządzanie dostępem do wielu kont AWS w ramach organizacji, z centralnym miejscem do zarządzania dostępem użytkowników.

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

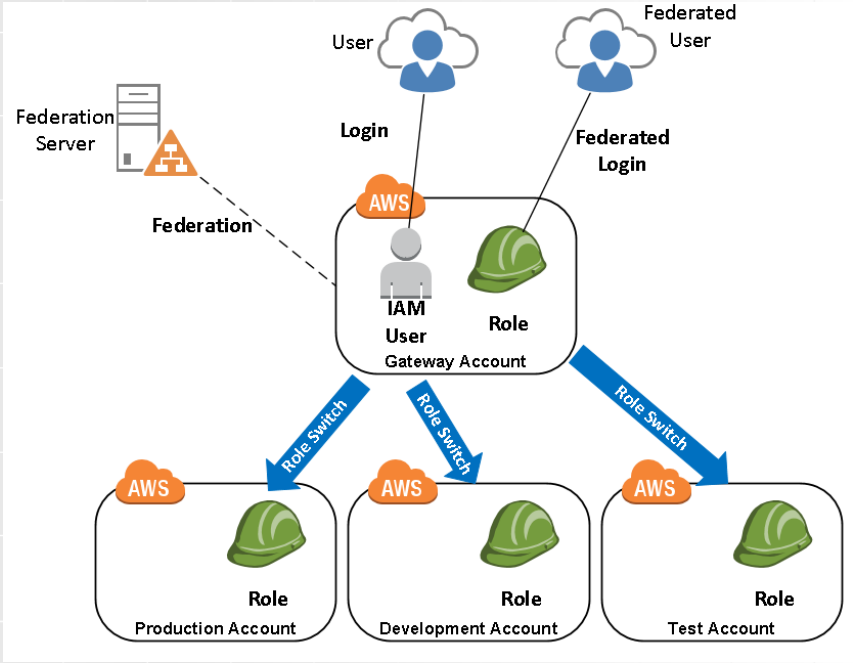


Użytkownik [2]

- Każdy użytkownik jest powiązany tylko z jednym kontem AWS
- Domyślnie nowo utworzony użytkownik nie ma uprawnień do wykonywania żadnej akcji w AWS
- Zaletą specyfikacji jeden-do-jednego użytkownika jest możliwość indywidualnego przypisywania uprawnień każdemu użytkownikowi

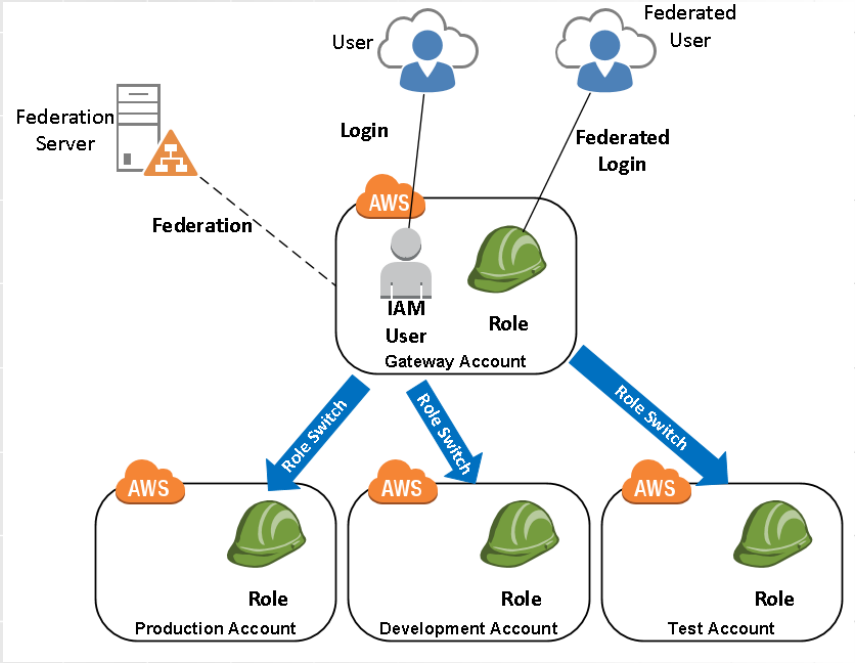
Rola [1]

- 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



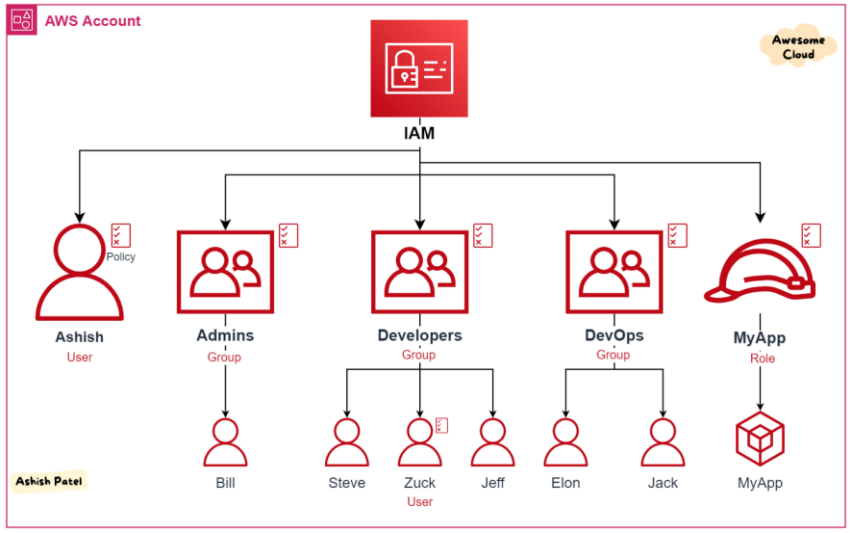
Rola [2]

- 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.



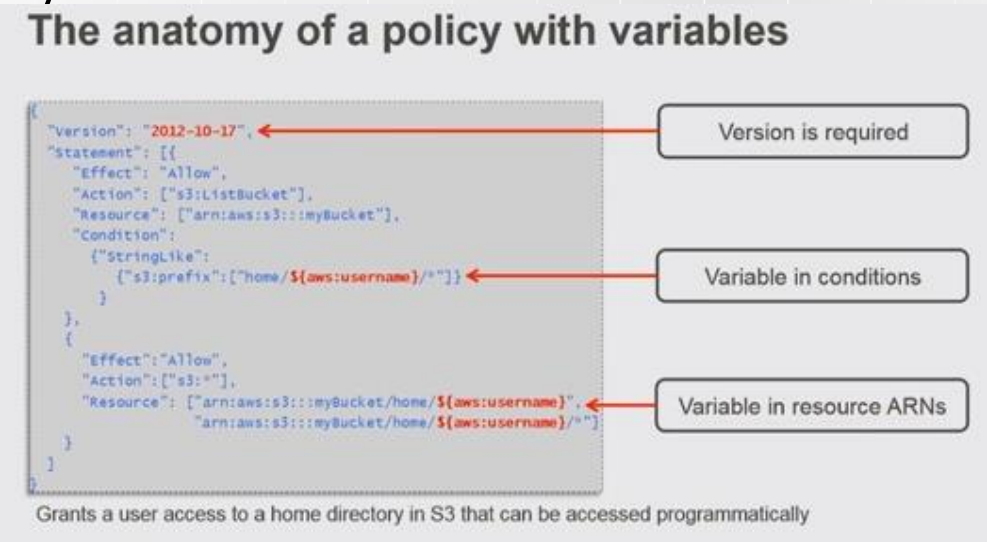
Grupa

- 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

Zarządzanie uprawnieniami: Użytkownik vs Rola

- 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

Wrocław University of Science and Technology

IAM

Wrocław University of Science and Technology

Billing

Wrocław
University
of Science
and Technology

Dziękuję za uwagę