Strategia zarządzania dostępem w AWS

2020 SOFTPROM *softprom.com* | *info@softprom.com* **Amazon Web Services Partner Network ADVANCED CONSULTING PARTNER** —

Użytkownicy: twórz indywidualnych użytkowników (Users)

Zgodnie z najlepszymi praktykami bezpieczeństwa nie należy używać konta głównego (root account), ponieważ zapewnia ono pełny dostęp do wszystkich usług i zasobów. Przyznawaj użytkownikom minimalny zakres uprawnień niezbędny do wykonania ich zadań, co jest znane jako zasada najmniejszych uprawnień (least privilege).

W Twojej grupie znajdują się inne osoby, które mają zróżnicowane uprawnienia dostępu i autoryzacji. Korzystanie z użytkowników IAM ułatwia przypisywanie polityk do konkretnych użytkowników uzyskujących dostęp do określonych usług i powiązanych z nimi zasobów.

- Użytkownik IAM może korzystać z AWS CLI.
- Użytkownik IAM może przyjmować role (roles).

Poniższy diagram opisuje standardowy przypadek użycia dla tworzenia użytkownika IAM:

1. **Utwórz użytkownika** (*Create user*).
2. **Przekaż użytkownikowi poświadczenia bezpieczeństwa** (*Give user security credentials*).
3. **Przypisz użytkownika do jednej lub kilku grup** (*Put user into one or more groups*).
4. **Opcjonalnie: Skonfiguruj profil logowania użytkownika** (*Give user a login profile - optional*).

Grupy: zarządzaj uprawnieniami za pomocą grup (Groups)

Grupa to zbiór użytkowników IAM. Grupy umożliwiają przypisywanie uprawnień do kolekcji użytkowników, co znacznie ułatwia zarządzanie ich uprawnieniami. Na przykład możesz utworzyć grupę o nazwie *Admins* i nadać jej uprawnienia, których zazwyczaj potrzebują administratorzy. Każdy użytkownik należący do tej grupy automatycznie otrzymuje przypisane do niej uprawnienia.

Jeśli do organizacji dołącza nowy pracownik i powinien otrzymać uprawnienia administratora, wystarczy dodać go do tej grupy. Podobnie, jeśli ktoś zmienia stanowisko w organizacji, zamiast edytować uprawnienia konkretnego użytkownika, można go po prostu usunąć ze starej grupy i dodać do nowej.

Uprawnienia: przypisuj minimalne przywileje (Permissions)

Aby przypisać uprawnienia dla użytkownika, grupy, roli lub zasobu, należy utworzyć politykę (policy), która pozwala zdefiniować następujące elementy:

- **Actions (Działania):** Dozwolone działania w ramach usługi AWS. Na przykład można pozwolić użytkownikowi na wywołanie działania `ListBucket` w usłudze Amazon S3. Wszelkie działania, które nie zostały wyraźnie dozwolone, są domyślnie zabronione.
- **Resources (Zasoby):** Zasoby AWS, na których dozwolone jest wykonywanie określonych działań. Na przykład lista kubełków Amazon S3, dla których zezwalasz użytkownikowi na wykonywanie działania `ListBucket`. Użytkownicy nie mają dostępu do zasobów, do których uprawnienia nie zostały wyraźnie przyznane.
- **Effect (Skutek):** Zezwolenie (*Allow*) lub odmowa (*Deny*) dostępu. Ponieważ domyślnie dostęp jest zablokowany, zazwyczaj tworzy się reguły, które jawnie zezwalają na określone działania.
- **Conditions (Warunki):** Warunki, które muszą zostać spełnione, aby polityka miała zastosowanie. Na przykład można zezwolić na dostęp do określonych kubełków S3 tylko wtedy, gdy użytkownik łączy się z określonego zakresu adresów IP lub używa uwierzytelniania wieloskładnikowego (MFA) podczas logowania.

Polityki są tworzone za pomocą edytora wizualnego lub bezpośrednio w formacie JSON. Polityka składa się z jednego lub kilku wyrażeń (statements), z których każde opisuje jeden zestaw uprawnień. Więcej informacji o języku reguł można znaleźć w dokumentacji dotyczącej polityk AWS IAM.

Edytor wizualny prowadzi użytkownika przez proces przyznawania uprawnień za pomocą reguł IAM bez konieczności samodzielnego pisania kodu w formacie JSON (przy czym możliwość tworzenia i edytowania reguł w formacie JSON pozostaje dostępna). Reguła przedstawiona w poniższym podsumowaniu została utworzona za pomocą edytora wizualnego. Przyznaje ona uprawnienia do pięciu działań Amazon S3 typu *List* i *Read* dla kubełka S3 oraz obiektów w `SampleBucket`, których prefiks zaczyna się od `MyPrefix`.

Przykład konfiguracji polityki (S3 - 5 działań):

- **Service (Usługa):** S3
- **Actions (Działania):**
  - **List:** `HeadBucket`, `ListAllMyBuckets`, `ListBucket`, `ListObjects`
  - **Read:** `GetObject`
- **Resources (Zasoby):**
  - `arn:aws:s3:::SampleBucket/*`
  - `arn:aws:s3:::SampleBucket`
- **Request Conditions (Warunki żądania):** `s3:prefix (StringEquals "MyPrefix")`

Korzystając z Konsoli zarządzania AWS do zarządzania uprawnieniami, można przeglądać zbiorcze podsumowanie reguły. W podsumowaniu wymienione są poziomy dostępu, zasoby

oraz warunki dla każdej usługi zdefiniowanej w polityce. Aby ułatwić zrozumienie uprawnień określonych w regule, działania każdej usługi AWS są podzielone na cztery kategorie według poziomu dostępu: *List*, *Read*, *Write* oraz *Permissions management*.

Service	Access level	Resource	Request condition
Allow (10 of 94 services)			
CloudFormation	Full List Limited: Read, Write	All resources	None
CloudWatch Logs	Full access	Multiple	None
EC2	Full List Limited: Read	All resources	None
Elastic Beanstalk	Full access	All resources	elasticbeanstalk:InApplication = arn:aws:elasticbeanstalk:111122223333:application/Bank-Dev

Możesz wybrać predefiniowaną regułę zarządzaną przez AWS (AWS Managed Policy) lub utworzyć własną, korzystając z generatora polityk. Więcej szczegółów znajduje się w sekcji *Omówienie polityk IAM* w Podręczniku użytkownika IAM.

Audyt: włącz usługę AWS CloudTrail

AWS CloudTrail umożliwia śledzenie historii konta i automatyczne reagowanie na działania zagrażające bezpieczeństwu używanych zasobów AWS. Dzięki integracji z *Amazon CloudWatch Events* można zdefiniować procesy robocze (workflows), które mają być uruchamiane w przypadku wykrycia zdarzeń mogących prowadzić do luk w zabezpieczeniach.

Na przykład można utworzyć proces, który automatycznie przypisze restrykcyjną politykę do kubełka Amazon S3, gdy CloudTrail wykryje wywołanie API otwierające publiczny dostęp do tego kubełka.

Hasło: skonfiguruj politykę wymagań dotyczących silnych haseł

Zarządzanie poświadczeniami za pomocą IAM

Usługa AWS Identity and Access Management (IAM) pozwala na zarządzanie kilkoma typami długoterminowych poświadczeń w celu zapewnienia bezpiecznego dostępu użytkowników IAM:

- **Hasła (Passwords):** Używane do logowania się na zabezpieczone strony AWS, takie jak Konsola zarządzania AWS czy fora AWS.
- **Klucze dostępu (Access Keys):** Używane do wykonywania programistycznych żądań do AWS za pośrednictwem API AWS, AWS CLI, AWS SDK lub narzędzi AWS dla Windows PowerShell.
- **Pary kluczy Amazon CloudFront (CloudFront Key Pairs):** Używane w CloudFront do tworzenia podpisanych adresów URL (signed URLs).
- **Klucze publiczne SSH (SSH Public Keys):** Używane podczas uwierzytelniania w repozytoriach AWS CodeCommit.

Przypisanie poświadczeń dostępu do zasobów AWS dla użytkowników IAM może odbywać się za pomocą API, interfejsu wiersza poleceń (CLI) lub Konsoli zarządzania AWS. Można rotować i unieważniać poświadczenia dostępu, gdy zajdzie taka potrzeba.

Oprócz zarządzania poświadczeniami użytkowników można dodatkowo zwiększyć bezpieczeństwo dostępu użytkowników IAM do zasobów AWS poprzez wymuszenie stosowania uwierzytelniania wieloskładnikowego (MFA).

Tymczasowe poświadczenia dostępu (Temporary Credentials)

IAM umożliwia również przyznawanie użytkownikom tymczasowych poświadczeń dostępu do zasobów AWS o określonym terminie ważności. Korzystanie z dostępu tymczasowego jest przydatne w następujących przypadkach:

- Tworzenie aplikacji mobilnej wykorzystującej logowanie za pośrednictwem zewnętrznych dostawców tożsamości.
- Tworzenie aplikacji mobilnej z własnym uwierzytelnianiem.
- Wykorzystanie wewnętrznego systemu uwierzytelniania organizacji do przyznawania dostępu do zasobów AWS.
- Wykorzystanie wewnętrznego systemu uwierzytelniania organizacji oraz standardu SAML do przyznawania dostępu do zasobów AWS.
- Korzystanie z logowania jednokrotnego (SSO) przez interfejs webowy do Konsoli zarządzania AWS.
- Delegowanie dostępu do API dla podmiotów zewnętrznych w celu odpytywania zasobów na Twoim koncie lub na innym posiadanym przez Ciebie koncie.

MFA: włącz uwierzytelnianie MFA dla użytkowników uprzywilejowanych

AWS Multi-Factor Authentication (MFA) to prosta i najlepsza praktyka, która dodaje dodatkową warstwę ochrony do nazwy użytkownika i hasła. Przy włączonym MFA, gdy użytkownik loguje się do Konsoli zarządzania AWS, zostanie poproszony o podanie nazwy użytkownika i hasła (pierwszy składnik — to, co wie), a także kodu uwierzytelniającego ze swojego urządzenia AWS MFA (drugi składnik — to, co posiada). Te wielokrotne składniki razem zapewniają zwiększone bezpieczeństwo ustawień i zasobów konta AWS.

Możesz włączyć MFA dla swojego konta AWS oraz dla poszczególnych użytkowników IAM utworzonych w ramach tego konta. MFA może być również używane do kontrolowania dostępu do API usług AWS.

Po uzyskaniu obsługiwanego sprzętowego lub wirtualnego urządzenia MFA, AWS nie pobiera żadnych dodatkowych opłat za korzystanie z funkcji MFA.

Można również chronić dostęp międzykontowy (cross-account access) za pomocą MFA.

Wirtualne aplikacje MFA (Virtual MFA Applications)

Aplikacje na smartfona można zainstalować ze sklepu z aplikacjami właściwego dla danego typu telefonu. Poniższa tabela przedstawia niektóre aplikacje dla różnych typów smartfonów.

System operacyjny	Obsługiwane aplikacje MFA
Android	Authy, Duo Mobile, LastPass Authenticator, Microsoft Authenticator, Google Authenticator
iPhone	Authy, Duo Mobile, LastPass Authenticator, Microsoft Authenticator, Google Authenticator

Klucz bezpieczeństwa U2F (U2F Security Key)

AWS obsługuje klucz bezpieczeństwa U2F jako urządzenie MFA do uzyskiwania dostępu do Konsoli zarządzania AWS przy użyciu określonych przeglądarek internetowych. Zachęcamy do korzystania z wirtualnego lub sprzętowego MFA dla aplikacji mobilnej AWS Console Mobile App. Więcej informacji można znaleźć w konfiguracjach związanych z kluczami bezpieczeństwa U2F obsługiwanymi przez AWS.

Role: używaj ról IAM dla instancji Amazon EC2

Role IAM pozwalają na przyznanie praw dostępu użytkownikom lub usługom, które zazwyczaj nie mają dostępu do zasobów AWS Twojej organizacji. Użytkownikom IAM lub usługom AWS można przypisać role w celu uzyskania tymczasowych poświadczeń dostępu, których mogą używać do wywołań API AWS. W rezultacie nie ma potrzeby przekazywania długoterminowych poświadczeń ani konfigurowania uprawnień dla każdego obiektu wymagającego dostępu do określonego zasobu.

Poniższe scenariusze wyróżniają wybrane problemy, z którymi można się spotkać podczas delegowania dostępu:

- **Przyznawanie aplikacjom działającym na instancjach Amazon EC2 dostępu do zasobów AWS:** Aby zapewnić aplikacjom na instancji Amazon EC2 dostęp do zasobów AWS, programiści mogliby umieścić swoje poświadczenia dostępu na każdej instancji. Aplikacje mogłyby wtedy używać tych danych do uzyskiwania dostępu do zasobów, takich jak kubełki Amazon S3 lub dane Amazon DynamoDB. Jednak udostępnianie długoterminowych poświadczeń każdej instancji jest kwestią dyskusyjną i stwarza potencjalne zagrożenie bezpieczeństwa. Role IAM pozwalają rozwiązać ten problem w bezpieczny sposób.
- **Dostęp do wielu kont:** Do kontpolowania lub zarządzania dostępem do zasobów — na przykład w celu odizolowania środowiska produkcyjnego od środowiska programistycznego — może być wymaganych wiele kont AWS. Jednak w niektórych przypadkach użytkownicy z jednego konta mogą potrzebować dostępu do zasobów innego konta. Na przykład użytkownik ze środowiska programistycznego może potrzebować dostępu do środowiska produkcyjnego w celu wdrożenia aktualizacji. Tradycyjnie użytkownicy musieliby posiadać osobne poświadczenia dla każdego konta, co utrudnia centralne zarządzanie tożsamościami. Użycie roli IAM upraszcza to zadanie.
- **Przyznawanie uprawnień usługom AWS:** Zanim usługi AWS będą mogły wykonywać jakiekolwiek działania w Twoim imieniu, musisz przyznać im odpowiednie uprawnienia. Możesz użyć ról AWS IAM, aby zezwolić usługom AWS na wywoływanie innych usług AWS w Twoim imieniu lub na tworzenie zasobów AWS i zarządzanie nimi na Twoim koncie. Usługi AWS, takie jak Amazon Lex, oferują również role powiązane z usługami (*service-linked roles*), które są wstępnie skonfigurowane i mogą być przyjmowane wyłącznie przez tę konkretną usługę.

Wspólny dostęp: używaj ról IAM do udostępniania zasobów (Federation)

Federacja tożsamości (identity federation) to system zaufania pomiędzy dwiema stronami w celu uwierzytelniania użytkowników i przekazywania informacji niezbędnych do autoryzacji ich dostępu do zasobów. W tym systemie dostawca tożsamości (Identity Provider - IdP) odpowiada za uwierzytelnianie użytkowników, a dostawca usług (Service Provider - SP), taki jak usługa lub aplikacja, kontroluje dostęp do zasobów. Na mocy umowy administracyjnej i konfiguracji, SP ufa

IdP w kwestii uwierzytelniania użytkowników i polega na dostarczanych przez IdP informacjach na ich temat.

Po uwierzytelnieniu użytkownika, IdP wysyła do SP komunikat, zwany asercją (assertion), zawierający nazwę logowania użytkownika oraz inne atrybuty, których SP potrzebuje do ustanowienia sesji z użytkownikiem i określenia zakresu dostępu do zasobów, jaki powinien mu przyznać. Federacja jest powszechnym podejściem do budowania systemów kontroli dostępu, które zarządzają użytkownikami centralnie w ramach głównego IdP i sterują ich dostępem do wielu aplikacji i usług działających jako SP.

AWS oferuje odrębne rozwiązania do federacji pracowników, kontrahentów i partnerów (workforce) z kontami AWS i aplikacjami biznesowymi, a także do dodawania obsługi federacji w aplikacjach internetowych i mobilnych skierowanych do klientów. AWS obsługuje powszechnie stosowane otwarte standardy tożsamości, w tym Security Assertion Markup Language 2.0 (SAML 2.0), OpenID Connect (OIDC) oraz OAuth 2.0.

Włączanie federacyjnego dostępu do AWS dla pracowników (Workforce)

Możesz użyć dwóch usług AWS do federacji swoich pracowników z kontami AWS i aplikacjami biznesowymi: *AWS Single Sign-On (SSO)* lub *AWS Identity and Access Management (IAM)*. AWS SSO to doskonały wybór, który pomaga definiować federacyjne uprawnienia dostępu dla użytkowników na podstawie ich członkostwa w grupach w jednym scentralizowanym katalogu. Jeśli korzystasz z wielu katalogów lub chcesz zarządzać uprawnieniami na podstawie atrybutów użytkowników, rozważ AWS IAM jako alternatywę projektową. Aby dowiedzieć się więcej o limitach usług i innych kwestiach projektowych w AWS SSO, zapoznaj się z Podręcznikiem użytkownika AWS SSO. W przypadku kwestii projektowych AWS IAM, zapoznaj się z Podręcznikiem użytkownika AWS IAM.

Wykorzystanie federacji do włączenia logowania jednokrotnego (SSO) do kont AWS

AWS SSO ułatwia centralne zarządzanie federacyjnym dostępem do wielu kont AWS i aplikacji biznesowych oraz zapewnia użytkownikom dostęp typu single sign-on do wszystkich przypisanych im kont i aplikacji z jednego miejsca. Możesz używać AWS SSO dla tożsamości w katalogu użytkowników AWS SSO, istniejącym katalogu korporacyjnym lub zewnętrznym IdP.

AWS SSO współpracuje z wybranym przez Ciebie IdP, takim jak *Okta Universal Directory* lub *Azure Active Directory (AD)* za pośrednictwem protokołu SAML 2.0. AWS SSO płynnie wykorzystuje uprawnienia i polityki IAM dla federacyjnych użytkowników i ról, pomagając centralnie zarządzać dostępem federacyjnym na wszystkich kontach AWS w Twojej organizacji AWS Organizations. Dzięki AWS SSO możesz przypisywać uprawnienia na podstawie członkostwa w grupach w katalogu dostawcy IdP, a następnie kontrolować dostęp dla swoich użytkowników, po prostu modyfikując użytkowników i grupy w IdP. AWS SSO obsługuje również standard System for Cross-domain Identity Management (SCIM) w celu umożliwienia automatycznego aprowizowania

(provisioning) użytkowników i grup z Okta Universal Directory, Azure AD i innych obsługiwanych IdP do AWS.

AWS SSO może służyć jako IdP do uwierzytelniania użytkowników w aplikacjach zintegrowanych z AWS SSO oraz w aplikacjach chmurowych zgodnych z SAML 2.0, takich jak Salesforce, Box i Office 365, z wybranym przez Ciebie katalogiem. Możesz także używać AWS SSO do uwierzytelniania użytkowników w Konsoli zarządzania AWS, aplikacji mobilnej AWS Console Mobile Application oraz interfejsie wiersza poleceń AWS CLI. Jako źródło tożsamości możesz wybrać Microsoft Active Directory lub katalog użytkowników AWS SSO.

Używanie AWS IAM do zarządzania precyzyjnym dostępem federacyjnym do kont AWS

Możesz włączyć dostęp federacyjny do kont AWS za pomocą AWS Identity and Access Management (IAM). Elastyczność AWS IAM pozwala na włączenie oddzielnego dostawcy IdP SAML 2.0 lub OpenID Connect (OIDC) dla każdego konta AWS i używanie federacyjnych atrybutów użytkowników do kontroli dostępu. Dzięki AWS IAM możesz przekazywać atrybuty użytkowników, takie jak centrum kosztów (cost center) lub rola zawodowa (job role), ze swoich dostawców IdP do AWS i wdrażać precyzyjne uprawnienia dostępu w oparciu o te atrybuty.

AWS IAM pomaga zdefiniować uprawnienia raz, a następnie przyznawać, cofać lub modyfikować dostęp do AWS poprzez prost