ORACLE

OCI IAM i rola MFA w bezpieczeństwie chmury

Przygotowano : 2025.09.03

Spis treści

ORACLE ..... **Błąd! Nie zdefiniowano zakładki.**
OCI IAM i rola MFA w bezpieczeństwie chmury ..... **Błąd! Nie zdefiniowano zakładki.**
Spis treści 2
OCI IAM i rola MFA w bezpieczeństwie chmury 3
Wprowadzenie do OCI Identity and Access Management (IAM) 3
Dlaczego OCI IAM jest tak ważny? 3
Czym jest MFA? 3
Jak działa MFA w OCI IAM? 4
Automatyczne włączenie MFA i polityki bezpieczeństwa 4
Zarządzanie i najlepsze praktyki MFA w OCI IAM 4

OCI IAM i rola MFA w bezpieczeństwie chmury

Wprowadzenie do OCI Identity and Access Management (IAM)

Oracle Cloud Infrastructure (OCI) Identity and Access Management (IAM) to kluczowa usługa, która pozwala na bezpieczne kontrolowanie dostępu do zasobów chmurowych. Jej głównym celem jest zarządzanie tożsamościami użytkowników, uwierzytelnianie (sprawdzanie, kim jest użytkownik) oraz autoryzacja (sprawdzanie, do jakich zasobów ma dostęp).

Podstawowe komponenty OCI IAM to:

- **Użytkownicy (Users):** Pojedyncze osoby lub tożsamości maszynowe, które mogą się uwierzytelniać i zarządzać zasobami.
- **Grupy (Groups):** Zbiory użytkowników, do których można przypisywać reguły dostępu. Ułatwia to zarządzanie, ponieważ uprawnienia nadaje się grupom, a nie pojedynczym użytkownikom.
- **Polityki (Policies):** Dokumenty określające, kto ma dostęp do jakich zasobów. Są to reguły zapisane w formacie Allow group <group-name> to <verb> <resource-type> in compartment <compartment-name>. Polityki są sercem kontroli dostępu w OCI.
- **Kompartmenty (Compartments):** Logiczne kontenery do grupowania i izolowania zasobów chmurowych. Pozwalają na precyzyjne definiowanie reguł dostępu dla poszczególnych działów, projektów czy środowisk (np. produkcja, testy).

Dlaczego OCI IAM jest tak ważny?

Odpowiednie zarządzanie tożsamością i dostępem w chmurze jest fundamentem bezpieczeństwa. Zapewnia, że tylko uprawnione osoby mogą modyfikować, przeglądać lub usuwać zasoby. Niewłaściwe skonfigurowanie uprawnień może prowadzić do naruszeń danych, uszkodzenia infrastruktury lub nieautoryzowanych kosztów. OCI IAM pomaga w osiągnięciu zgodności z regulacjami takimi jak RODO (GDPR) czy PCI DSS.

Czym jest MFA?

Multi-Factor Authentication (MFA) to metoda uwierzytelniania, która wymaga od użytkownika podania co najmniej dwóch różnych czynników uwierzytelniających. Standardowo pierwszym czynnikiem jest coś, co użytkownik zna (np. hasło). Drugim czynnikiem jest coś, co użytkownik posiada (np. token jednorazowy generowany na telefonie, powiadomienie push, klucz bezpieczeństwa), co znacząco podnosi poziom bezpieczeństwa. Dzięki temu nawet jeśli hasło zostanie przechwycone, ryzyko nieuprawnionego dostępu pozostaje minimalne.

Jak działa MFA w OCI IAM?

Po wprowadzeniu loginu i hasła (pierwszy czynnik), użytkownik zostaje poproszony o podanie drugiego czynnika do weryfikacji. Drugi czynnik może przyjmować różne formy:

- jednorazowe hasło (OTP) generowane przez aplikację mobilną (np. Google Authenticator, Microsoft Authenticator),
- powiadomienie push na urządzeniu mobilnym,
- sprzętowy klucz bezpieczeństwa (np. YubiKey),
- SMS z kodem weryfikacyjnym.

Wdrożenie MFA zabezpiecza dostęp do **OCI Console** oraz innych aplikacji i usług korzystających z OCI IAM.

Automatyczne włączenie MFA i polityki bezpieczeństwa

W 2023 roku Oracle wprowadziło domyślną politykę bezpieczeństwa o nazwie **„Security Policy For OCI Console”**, która automatycznie aktywuje MFA dla wszystkich użytkowników posiadających uprawnienia administracyjne w konsoli.

- Dla środowisk **IAM Identity Domains** polityka zaczęła być aktywowana od **17 lipca 2023 r.**
- Dla środowisk **Identity Cloud Service** – od **24 lipca 2023 r.**

Polityka ta dotyczy wyłącznie użytkowników lokalnych logujących się bezpośrednio do konsoli OCI.
Nie zostanie ona aktywowana automatycznie w sytuacjach, gdy:

- istnieje już zmodyfikowana domyślna polityka logowania,
- dostęp do konsoli jest regulowany inną polityką sign-on,
- skonfigurowano aktywnego zewnętrznego dostawcę tożsamości (np. Azure AD, Okta, federacja SAML lub X.509).

Dzięki temu organizacje korzystające z federacji mogą kontynuować stosowanie własnych reguł MFA skonfigurowanych w zewnętrznych IdP.

Zarządzanie i najlepsze praktyki MFA w OCI IAM

Aby w pełni wykorzystać możliwości MFA w OCI, Oracle rekomenduje:

- **Włączanie MFA dla wszystkich użytkowników** posiadających dostęp do konsoli OCI – nie tylko administratorów.

- **Preferowanie metod opartych na aplikacjach mobilnych np. Oracle Mobile Authenticator lub kluczach sprzętowych** zamiast SMS, które są bardziej podatne na ataki (np. SIM swap).
- **Regularne przeglądy i aktualizacje polityk dostępu** – szczególnie po zmianach organizacyjnych lub przy dodawaniu nowych aplikacji.
- **Monitorowanie użytkowników bez MFA** – w tym celu można korzystać z narzędzi takich jak **Oracle Cloud Guard**, które pozwalają identyfikować potencjalne luki bezpieczeństwa.
- **Integrację MFA z zewnętrznymi dostawcami tożsamości**, jeśli organizacja korzysta z federacji logowania (np. Microsoft Entra ID, Okta), co pozwala na centralne zarządzanie politykami bezpieczeństwa.

Jak skonfigurować MFA dla użytkownika w OCI IAM

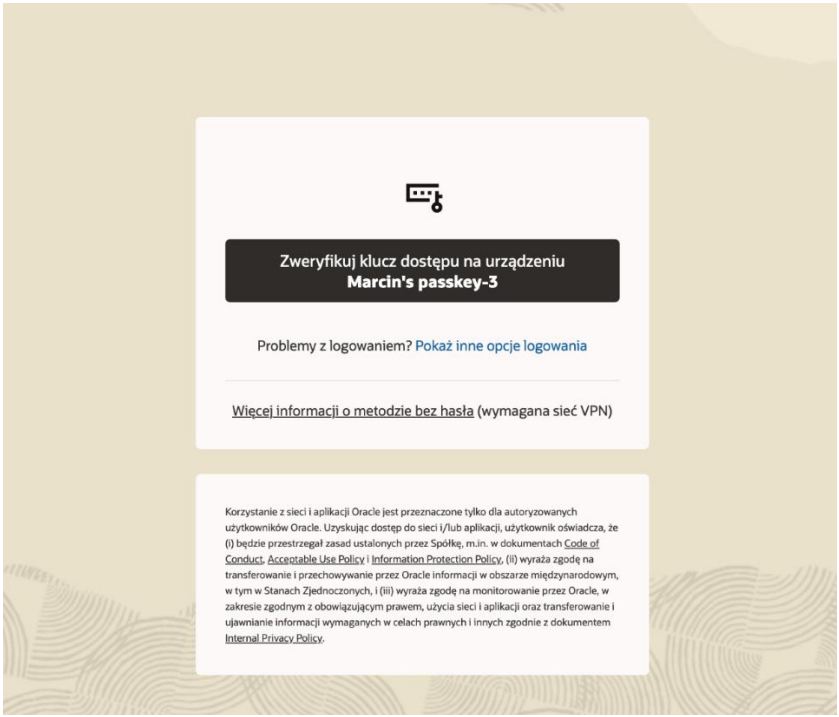
Możesz łatwo uruchomić MFA dla konkretnego użytkownika z poziomu konsoli OCI IAM:

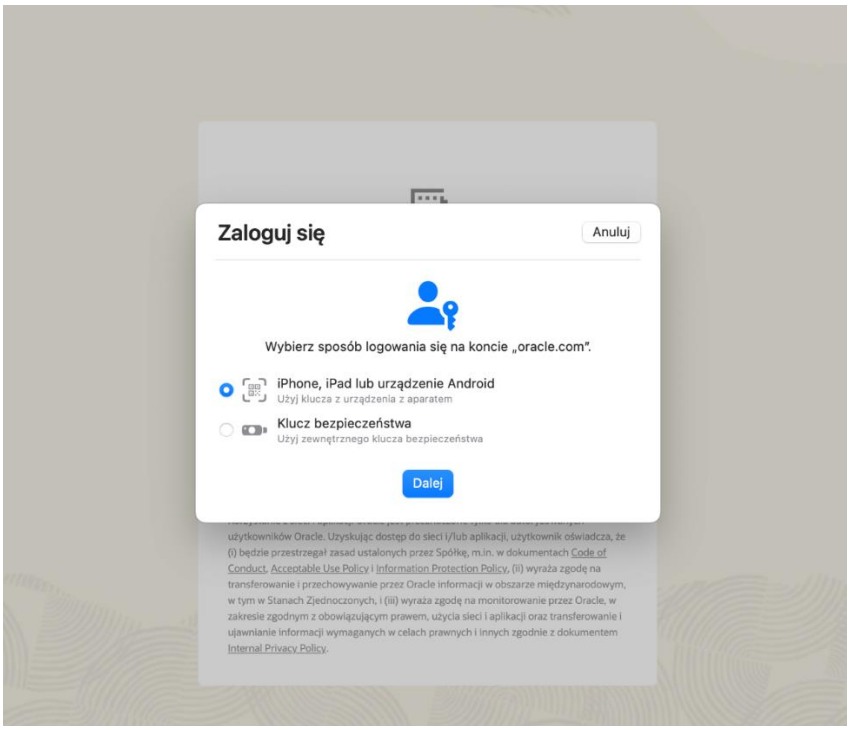
1. Zaloguj się do OCI Console jako użytkownik IAM.
2. Przejdź do Menu → Identity & Security → Identity → Users.
3. Wybierz użytkownika z listy lokalnych użytkowników IAM.
4. Kliknij opcję Enable Multi-Factor Authentication.
5. Zeskanuj kod QR przy użyciu wybranej aplikacji autoryzacyjnej (np. Google Authenticator, Microsoft Authenticator, Oracle Authenticator itp.).
6. Wprowadź kod, który wygenerowała aplikacja, co kończy proces rejestracji drugiego czynnika.
7. Po aktywacji, przy każdym logowaniu użytkownik będzie proszony o jednorazowy kod z aplikacji.

Oracle zaleca użycie:

- **Cloud Guard:** To usługa, która automatycznie skanuje i monitoruje środowisko OCI pod kątem naruszeń bezpieczeństwa, w tym braku włączonego MFA dla użytkowników. Korzystanie z Cloud Guard to najlepszy sposób na audyt i identyfikację ryzyk w zakresie tożsamości.
- **Zastosowanie polityk:** w zależności od tego, czy dana dzierżawa posiada już nową politykę, czy też nie, należy postępować zgodnie z odpowiednimi instrukcjami, aby zapewnić, że MFA jest aktywne dla wszystkich kluczowych użytkowników.


Logowanie do Oracle
Należy wprowadzić swój adres e-mail Oracle
test@mail.com
Dalej
Korzystanie z sieci i aplikacji Oracle jest przeznaczone tylko dla autoryzowanych użytkowników Oracle. Uzyskując dostęp do sieci i/lub aplikacji, użytkownik oświadcza, że (i) będzie przestrzegał zasad ustalonych przez Spółkę, m.in. w dokumentach Code of Conduct, Acceptable Use Policy i Information Protection Policy, (ii) wyraża zgodę na transferowanie i przechowywanie przez Oracle informacji w obszarze międzynarodowym, w tym w Stanach Zjednoczonych, i (iii) wyraża zgodę na monitorowanie przez Oracle, w zakresie zgodnym z obowiązującym prawem, użycia sieci i aplikacji oraz transferowanie i ujawnianie informacji wymaganych w celach prawnych i innych zgodnie z dokumentem Internal Privacy Policy.


Zweryfikuj klucz dostępu na urządzeniu
Marcin's passkey-3
Problemy z logowaniem? Pokaż inne opcje logowania
Więcej informacji o metodzie bez hasła (wymagana sieć VPN)
Korzystanie z sieci i aplikacji Oracle jest przeznaczone tylko dla autoryzowanych użytkowników Oracle. Uzyskując dostęp do sieci i/lub aplikacji, użytkownik oświadcza, że (i) będzie przestrzegał zasad ustalonych przez Spółkę, m.in. w dokumentach Code of Conduct, Acceptable Use Policy i Information Protection Policy, (ii) wyraża zgodę na transferowanie i przechowywanie przez Oracle informacji w obszarze międzynarodowym, w tym w Stanach Zjednoczonych, i (iii) wyraża zgodę na monitorowanie przez Oracle, w zakresie zgodnym z obowiązującym prawem, użycia sieci i aplikacji oraz transferowanie i ujawnianie informacji wymaganych w celach prawnych i innych zgodnie z dokumentem Internal Privacy Policy.



Przykład procesu logowania do **OCI z MFA / passkey**