

IBM Cloud Integrated Analytics Environment

Niniejszy opis dotyczy Usługi Przetwarzania w Chmurze, którą IBM oferuje Klientowi. „Klient” oznacza tu podmiot zawierający umowę wraz z jego autoryzowanymi użytkownikami i odbiorcami Usługi Przetwarzania w Chmurze. Odpowiednia Oferta Cenowa i dokument Proof of Entitlement (PoE) są dostarczane jako odrębne Dokumenty Transakcyjne.

1. Usługa Przetwarzania w Chmurze

IBM Cloud Integrated Analytics Environment (IAE) to model wdrażania, który zapewnia poufną, rodzimą łączność między różnymi aktywowanymi, oddzielnie nabywanymi Usługami Przetwarzania w Chmurze oraz udostępnia opcje umożliwiające bezpieczne łączenie się z urządzeniami klienckimi.

Klient musi nabyć następujące uprawnienia:

- IBM Cloud Integrated Analytics Environment lub IBM Cloud Integrated Analytics Dedicated Environment; oraz
- IBM Cloud Integrated Analytics VPN Connectivity, IBM Cloud Integrated Analytics Standard Security Appliance lub IBM Cloud Integrated Analytics Enterprise Security Appliance.

1.1 Usługi Podstawowe

1.1.1 IBM Cloud Integrated Analytics Environment

Środowisko IBM Cloud Integrated Analytics Environment jest wdrażane w centrum przetwarzania danych IBM SoftLayer. W jego skład wchodzi dwie strefy:

- Strefa Usług Zarządzanych, w której wdrażane są usługi zarządzane rodzime dla środowiska IAE (w tym zarządzane przez IBM sieci VPN typu serwer-serwer) oraz zarządzane usługi SaaS z rodziny IBM Analytics. Strefą tą zarządza IBM.
- Strefa Usług Udostępnianych na Serwerze, w której wdrażane są udostępniane na serwerze usługi SaaS z rodziny IBM Analytics. Mogą to być:
 - rozwiązania udostępniane na serwerze, takie jak DB2 on Cloud;
 - serwery IAE określone poniżej.

Strefa Usług Udostępnianych na Serwerze może być opcjonalnie chroniona zewnętrznym firewallem w postaci nabywanego oddzielnie i zarządzanego przez Klienta urządzenia IBM Cloud Integrated Analytics Standard Security Appliance lub IBM Cloud Integrated Analytics Enterprise Security Appliance.

1.1.2 IBM Cloud Integrated Analytics Dedicated Environment

Ta Usługa Przetwarzania w Chmurze udostępnia Klientom wszystkie funkcje usługi IBM Cloud Integrated Analytics Environment opisane powyżej, skonfigurowane z użyciem dedykowanych firewalli.

1.1.3 IBM Cloud Integrated VPN Connectivity

Zarządzana przez IBM usługa sieci VPN typu serwer-serwer. IBM automatycznie przerywa każde połączenie VPN po zakończeniu korzystania ze środowiska IBM Cloud Integrated Analytics Environment. Usługa IBM Cloud Integrated Analytics VPN Connectivity korzysta z technologii sieci VPN typu serwer-serwer zgodnej ze standardem IPsec.

1.1.4 IBM Cloud Integrated Analytics Standard Security Appliance

Dedykowane urządzenie zabezpieczające wdrażane w Strefie Usług Udostępnianych na Serwerze i zarządzane przez Klienta. Umożliwia Klientowi utworzenie zarządzanej przez Klienta sieci VPN typu serwer-serwer lub sieci VPN typu klient-serwer oraz oddzielenie Strefy Usług Udostępnianych na Serwerze od publicznego Internetu przy użyciu firewalla.

1.1.5 IBM Cloud Integrated Analytics Enterprise Security Appliance

Nadmiarowa para dedykowanych urządzeń zabezpieczających wdrażana w Strefie Usług Udostępnianych na Serwerze. Umożliwia utworzenie zarządzanej przez Klienta sieci VPN typu serwer-serwer lub sieci VPN typu klient-serwer oraz oddzielenie Strefy Usług Udostępnianych na Serwerze od publicznego Internetu przy użyciu firewalla.

1.2 Usługi Opcjonalne

1.2.1 Serwery IAE

Serwery środowiska IBM Cloud Integrated Analytics Environment wdrażane w Strefie Usług Udostępnianych na Serwerze, wykorzystywane do obsługi należących do Klienta aplikacji, które wymagają szybkich, charakteryzujących się małymi opóźnieniami połączeń z innymi aplikacjami w Strefie Usług Zarządzanych i Strefie Usług Udostępnianych na Serwerze.

- **IBM Cloud Integrated Analytics Extra Small Server**

Zarządzany przez Klienta serwer IBM SoftLayer charakteryzujący się co najmniej następującymi parametrami: 1 publiczny rdzeń wirtualny, 4 GB pamięci RAM, 25 GB miejsca na dysku w sieci SAN.

- **IBM Cloud Integrated Analytics Small Server**

Zarządzany przez Klienta serwer IBM SoftLayer charakteryzujący się co najmniej następującymi parametrami: 4 prywatne rdzenie wirtualne, 16 GB pamięci RAM, 100 GB miejsca na dysku w sieci SAN.

- **IBM Cloud Integrated Analytics Medium Server**

Zarządzany przez Klienta serwer IBM SoftLayer charakteryzujący się co najmniej następującymi parametrami: 8 prywatnych rdzeni wirtualnych, 32 GB pamięci RAM, 100 GB miejsca na dysku nr 1 w sieci SAN, 100 GB miejsca na dysku nr 2 w sieci SAN.

- **IBM Cloud Integrated Analytics Large Server**

Zarządzany przez Klienta serwer IBM SoftLayer charakteryzujący się co najmniej następującymi parametrami: 16 prywatnych rdzeni wirtualnych, 64 GB pamięci RAM, 100 GB miejsca na dysku nr 1 w sieci SAN, 100 GB miejsca na dysku nr 2 w sieci SAN.

- **IBM Cloud Integrated Analytics Storage**

Do serwerów IAE można dodawać pamięć masową w sieci SAN w pakietach po 100, 250 lub 500 GB.

2. Opis zabezpieczeń

W odniesieniu do niniejszej Usługi Przetwarzania w Chmurze nie są stosowane zasady ochrony danych i prywatności dla Usług Przetwarzania w Chmurze. Usługa Przetwarzania w Chmurze jest kontrolowana przez Klienta, który ma obowiązek zapewnić jej zgodność z własnymi standardami bezpieczeństwa. Klient przyjmuje do wiadomości, że niniejsza Usługa Przetwarzania w Chmurze nie oferuje funkcji ochrony zawartości obejmującej dane osobowe, wrażliwe dane osobowe oraz dane podlegające dodatkowym wymaganiom prawnym. Jeśli Klient umieści takie dane w swojej zawartości, poinstruuje IBM, aby były one przetwarzane zgodnie z niniejszą Umową po ustaleniu, że techniczne i organizacyjne środki bezpieczeństwa są odpowiednie do czynników ryzyka związanych z przetwarzaniem i rodzajem danych podlegających ochronie. Klient przyjmuje do wiadomości, że IBM nie dysponuje wiedzą na temat typów danych znajdujących się w takiej zawartości i nie jest w stanie dokonać oceny przydatności Usług Przetwarzania w Chmurze ani zastosowanych środków ochrony.

2.1 Opcje zabezpieczające i obowiązki związane z bezpieczeństwem

W Usłudze Przetwarzania w Chmurze zaimplementowano następujące opcje zabezpieczające:

Niniejsza Usługa Przetwarzania w Chmurze szyfruje zawartość podczas transmisji poza sieć IBM. Nie szyfruje natomiast zawartości, która znajduje się w stanie spoczynku i oczekuje na transmisję danych. Klient odpowiada za szyfrowanie zawartości przed jej dodaniem do Usługi Przetwarzania w Chmurze.

IBM ma obowiązek powiadamiać Klienta o incydentach związanych z bezpieczeństwem, natomiast za badanie takich incydentów i usuwanie ich skutków odpowiada Klient. IBM zastrzega sobie prawo do odizolowania Usługi Przetwarzania w Chmurze i wstrzymania jej świadczenia w przypadku naruszenia jej ochrony w wyniku incydentu, którego skutki nie zostały usunięte.

3. Wsparcie techniczne

Wsparcie techniczne do Usługi Przetwarzania w Chmurze jest świadczone za pośrednictwem forów internetowych oraz elektronicznego systemu zgłaszania problemów. IBM udostępni „Podręcznik wsparcia dla usługi IBM Software as a Service (SaaS)”, który zawiera informacje kontaktowe działu wsparcia

technicznego oraz inne informacje i procesy. Wsparcie techniczne jest oferowane razem z Usługą Przetwarzania w Chmurze i nie jest dostępne jako oddzielna oferta.

4. Informacje o uprawnieniach i rozliczaniu

4.1 Opłaty rozliczeniowe

Przy sprzedaży Usługi Przetwarzania w Chmurze wysokość opłat rozliczeniowych jest ustalana na podstawie jednej z następujących miar określonych w Dokumencie Transakcyjnym:

Jednostką miary, według której można korzystać z Usługi Przetwarzania w Chmurze, jest Instancja. Instancja oznacza dostęp do konkretnej konfiguracji Usługi Przetwarzania w Chmurze. Dla każdej udostępnionej Instancji Usługi Przetwarzania w Chmurze Klient musi uzyskać odpowiednie uprawnienia umożliwiające mu uzyskiwanie do niej dostępu i jej używanie w okresie pomiarowym określonym w dokumencie PoE lub Dokumencie Transakcyjnym Klienta.

Jednostką miary, według której można korzystać z Usługi Przetwarzania w Chmurze, jest Gigabajt. Gigabajt definiuje się jako 2 do 30. potęgi bajtów danych (1 073 741 824 bajty). Klient musi uzyskać odpowiednie uprawnienia umożliwiające obsługę łącznej liczby Gigabajtów przetwarzanych przez Usługę Przetwarzania w Chmurze w okresie pomiarowym określonym w dokumencie PoE lub Dokumencie Transakcyjnym Klienta.

5. Okres obowiązywania i możliwości odnowienia

Okres obowiązywania Usługi Przetwarzania w Chmurze rozpoczyna się z datą powiadomienia Klienta przez IBM o udostępnieniu mu tej usługi zgodnie z dokumentem PoE. W dokumencie PoE zostanie określone, czy Usługa Przetwarzania w Chmurze będzie odnawiana automatycznie, kontynuowana na zasadzie nieprzerwanego używania czy zakończona po upływie okresu jej obowiązywania.

W przypadku odnawiania automatycznego Usługa Przetwarzania w Chmurze będzie automatycznie przedłużana na okres wskazany w dokumencie PoE, chyba że Klient złoży pisemny wniosek o jej nieprzedłużanie co najmniej 90 dni przed datą jej wygaśnięcia.

W przypadku kontynuacji na zasadzie nieprzerwanego używania dostępność Usługi Przetwarzania w Chmurze będzie przedłużana z miesiąca na miesiąc, chyba że Klient wypowie ją pisemnie z wyprzedzeniem co najmniej 90 dni. Po zakończeniu takiego 90-dniowego okresu wypowiedzenia Usługa Przetwarzania w Chmurze będzie dostępna do końca miesiąca kalendarzowego.

6. Warunki dodatkowe

6.1 Postanowienia ogólne

Klient wyraża zgodę na publikowanie przez IBM w komunikatach reklamowych lub marketingowych informacji o Kliencie jako subskrybencie Usług Przetwarzania w Chmurze.

6.2 Zobowiązania Klienta

Wypełnienie kwestionariusza dotyczącego wirtualnej sieci prywatnej (VPN) i odesłanie go do IBM w celu weryfikacji przed datą rozpoczęcia konfigurowania sieci VPN.

Wyznaczenie osoby kontaktowej ds. technicznych, która dysponuje wiedzą na temat sieci korporacyjnej i sieci VPN Klienta oraz jego wymagań w zakresie bezpieczeństwa.

Zapewnienie dostępności administratora zabezpieczeń i sieci, który będzie współpracować z IBM przy konfigurowaniu sieci VPN (w fazie konfigurowania i sprawdzania poprawności konfiguracji sieci VPN).

Wykonywanie wszystkich czynności związanych z serwisowaniem, modyfikowaniem, konfigurowaniem i testowaniem sprzętu i oprogramowania oraz administrowaniem nimi w ośrodku Klienta wykorzystywanym do obsługi sieci VPN.

Przeprowadzanie testów reakcji użytkowników w celu sprawdzenia poprawności konfiguracji sieci VPN podczas wdrażania.

Powiadamianie za pośrednictwem elektronicznego systemu zgłaszania problemów o wszelkich niezbędnych zmianach konfiguracji sieci VPN.