

Novell Cloud Security Service

Realizowanie obietnic związanych z Cloud Computing

Novell.

Wprowadzenie

Novell Cloud Security Service jest opartym na sieci rozwiązaniem do bezpiecznego zarządzania zasobami oraz dostępem, dzięki któremu dostawcy rozwiązań cloud wraz z usługami SaaS (*software as a service*), PaaS (*platform as a service*) i IaaS (*infrastructure as a service*) mogą zapewnić większe bezpieczeństwo swoim klientom.

Rozwiązania cloud umożliwiają łatwe poszerzenie posiadanego centrum danych do przestrzeni typu cloud, co wpływa na lepsze wykorzystanie zasobów oraz obniżenie kosztów związanych z IT. Choć wiele przedsiębiorstw potwierdza zalety korzystania z cloud computing, to jednak niechętnie przenoszą przetwarzanie czy przechowywanie danych do przestrzeni typu cloud nie mając gwarancji, że procesy te będą odpowiednio zabezpieczone przez dostawcę tych usług. Podczas ostatniej konferencji RSA John Chambers, dyrektor generalny Cisco Systems, przyznał, że posunięcie przemysłu IT w stronę sprzedaży „pay-as-you-go”, usługi dostępnej w Internecie, pod względem bezpieczeństwa okazało się „koszmarem”, którego nie da się rozwiązać w tradycyjny sposób¹.

Upraszczając, bezpieczeństwo danych w środowisku typu cloud jest dla przedsiębiorstw rzeczą najważniejszą, co zostało potwierdzone w licznych ankietach dotyczących rozwiązań cloud computing. W ankietach bezpieczeństwo jest wielokrotnie wymieniane jako najważniejszy powód, dla którego przedsiębiorstwa nie decydują się na przetwarzanie czy przechowywanie danych w przestrzeni cloud. Przedsiębiorcy wyrażają również obawy co do braku umiejętności przydzielania i zarządzania dostępem do zasobów znajdujących się w przestrzeni cloud.

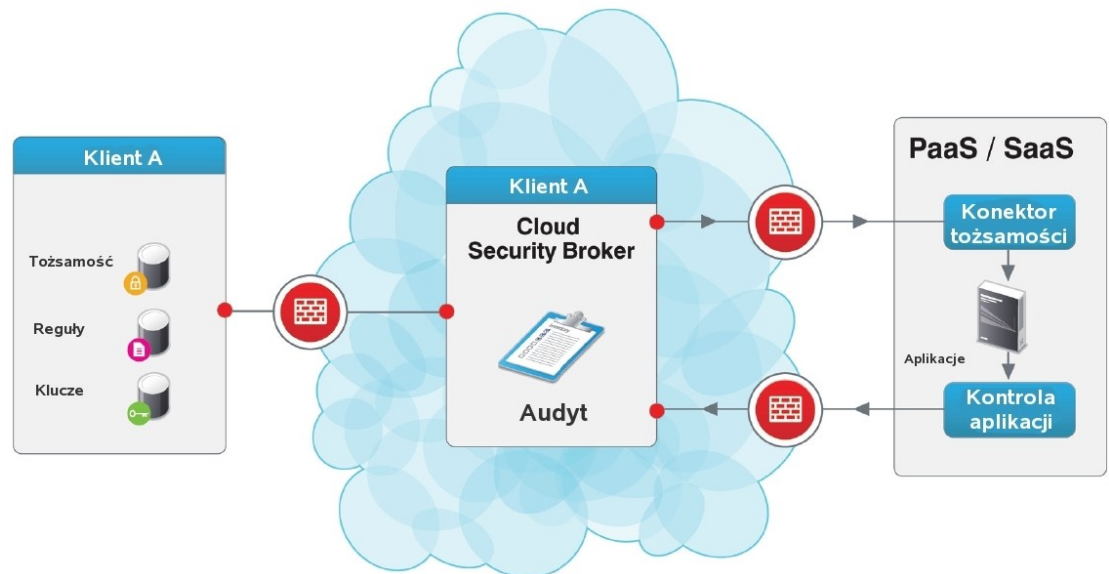
Oprogramowanie Novell Cloud Security Service podchodzi do problemu z perspektywy dostawcy rozwiązań cloud. Cloud Security Service odgrywa rolę zaufanego pośrednika pomiędzy przedsiębiorstwem a dostawcą rozwiązań cloud, pozwalając przedsiębiorcom na bezpieczne korzystanie z zasobów informatycznych w przestrzeni cloud. Cloud Security Service wprowadza bezpieczeństwo w środowisku cloud w unikalny sposób, zwany inkorporacją (ang. *annexing*), czyli poprzez rozciągnięcie zakresu praktyk, reguł biznesowych i działań przedsiębiorstwa do przestrzeni cloud. Inkorporacja umożliwia ujednoczony wgląd do zasobów cloud, umożliwiając jednolity dostęp oraz zarządzanie niezależnie od miejsca, z którego użytkownik korzysta z przestrzeni cloud. Takie podejście zapewnia, że działania biznesowe i operacyjne przedsiębiorstwa mogą być jednolite dla środowiska cloud oraz dla centrum danych.

Novell Cloud Security Service umożliwia również integrację obciążeń (rozumianych jako usługi działające na serwerach) w obrębie przestrzeni objętej wzmoczoną ochroną dzięki opatentowanej technologii przekazującej informacje dotyczące tożsamości oraz audytu pomiędzy obciążeniami, bez potrzeby wprowadzania do nich jakichkolwiek zmian.

Ponadto Cloud Security Service zarządza kluczami kryptograficznymi w celu zapewnienia bezpieczeństwa informacji, zarówno przechowywanych, jak i przenoszonych „z” oraz „do” przestrzeni cloud. Klucze kryptograficzne są lepiej zabezpieczone, ponieważ nie przechowuje się ich w przestrzeni cloud. Generowanie, wymiana i przechowywanie kluczy kontrolowane jest przez przedsiębiorstwo, a w przestrzeni cloud nie można przechowywać żadnych informacji bez wystosowania specjalnego polecenia od personelu zarządzającego centrum danych.

¹ Computerworld: „Rozwiązania typu cloud to koszmar pod względem bezpieczeństwa – mówi dyrektor generalny Cisco Systems.” Kwiecień 2009.

Novell Cloud Security Service stanowi brakujący element zabezpieczeń i pozwala rozwiązaniom typu cloud na zaistnienie w przedsiębiorstwach na całym świecie.



Ilustracja 1. Novell Cloud Security Service w przestrzeni cloud.

Jak działa Novell Cloud Security Service

Przedsiębiorstwo (Klient A) chce skorzystać z usług dostawcy SaaS² posiadającego rozwiązanie Novell Cloud Security Service. W tym przypadku użytkownik u Klienta A może zalogować się do Cloud Security Service bezpośrednio lub poprzez system zarządzający tożsamością użytkowników, jeżeli taki jest posiadany przez przedsiębiorcę. Na wstępie Cloud Security Broker weryfikuje tożsamość użytkownika z przedsiębiorstwem. Jeżeli użytkownik jest uprawniony, pośrednik (broker) generuje i podaje token uwierzytelniający w formacie wybranym przez dostawcę rozwiązań cloud.

Kluczowe komponenty Novell Cloud Security Service oraz ich działanie zostały opisane poniżej.

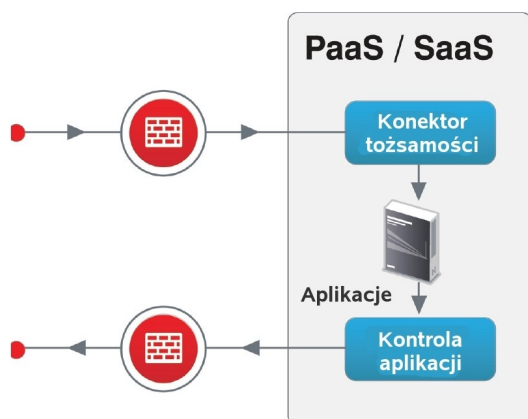
Komunikacja z dostawcami usług SaaS i PaaS

Novell udostępnia usługi Platform as a Service (PaaS)³ i Software as a Service (SaaS) wraz z powiązaniem konektorem tożsamości i konektorem zdarzeń. Konektory te są charakterystyczne dla danej platformy lub infrastruktury do świadczenia usług udostępnionych przez sprzedawcę. W przypadku braku konektora, Novell we współpracy z dostawcą rozwiązań udzieli pomocy w tworzeniu powiązanego konektora tożsamości oraz konektora zdarzeń dla każdej platformy PaaS lub SaaS. Novell posiada już gotowe konektory dla popularnych usług jak Salesforce.com, Google Apps, narzędzi do budowy aplikacji, jak Spring czy aplikacji jak Microsoft SharePoint.

² Dostawca usług SaaS: na przykład, Salesforce.com lub Google Apps

³ Dostawca usług PaaS: na przykład, Force.com or Google App Engine

W większości przypadków sama platforma udostępniona przez dostawców usług PaaS jest już wystarczająco wszechstronna, aby dostarczyć mechanizmy obsługi tożsamości, audytu i zapewnienia zgodności i tym samym umożliwia inkorporację PaaS.

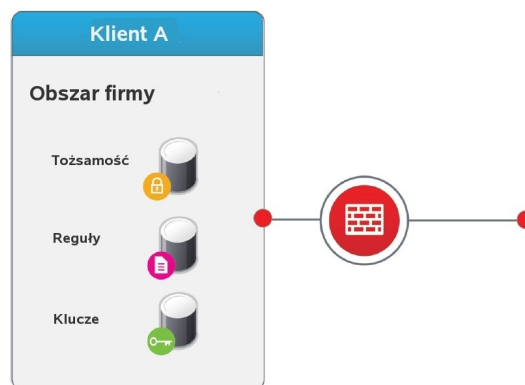


Środowisko SaaS może różnić się od środowiska PaaS z powodu braku wszechstronnej platformy. Jeżeli platforma nie jest wyeksponowana przez dostawcę usług SaaS, Cloud Security Service udostępniani wyspecjalizowane konektory dla usług SaaS. Kolejną opcją jest modyfikacja aplikacji w środowisku SaaS w celu bezpośredniego korzystania z interfejsu API dla Cloud Security Service, co wpłynie na zwiększenie wydajności. Novell Cloud Security Service traktuje obydwie opcje jako konieczne do wspierania użytkowników SaaS.

Ilustracja 2. Konektory tożsamości i konektory zdarzeń.

Łączność z przedsiębiorstwem

Novell zbudował gotowe do użycia konektory dla większości dostawców systemów do obsługi tożsamości, w tym firm IBM, Microsoft, CA, Oracle, Sun, Novell i innych. Zajmujący mało miejsca moduł wspierający stanowi bezpieczny, wdrożony lokalnie łącznik ze środowiskiem cloud, którym zarządza się z centrum danych (za zaporą). Łącznik ten udostępnia protokół proxy, agenta polityk, agenta audytu, menedżera bezpiecznej komunikacji oraz agenta kluczy. Protokół proxy jest protokołem o wielu zastosowaniach, który zezwala na agregację wielu protokołów do przyjaznych dla zapory pakietów (takich jak wysłane na port 443). Agent polityk i agent audytu pozwalają na dostarczenie informacji o zdarzeniach do wdrożonych lokalnie narzędzi do audytu i monitoringu. Z kolei agent polityk zapewnia bezpieczny dostęp do polityk przedsiębiorstwa z poziomu brokera (Cloud Security Broker), o ile przedsiębiorstwo nie posiada infrastruktury tożsamości, audytu, polityk oraz kluczy. Magazyny te mogą z łatwością być przechowywane w przestrzeni cloud w obrębie Cloud Security Service.



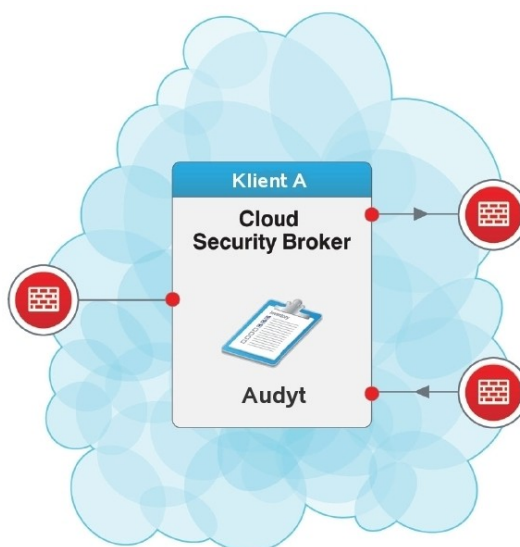
Ilustracja 3. Po stronie przedsiębiorstwa.

Novell Cloud Security Service pełni również funkcję administracyjną. Funkcja ta umożliwia jednolity podgląd wszystkich zasobów, które zostały udostępnione przez centrum danych jako część Cloud Security Service albo środowisko PaaS lub SaaS. Ponadto, Cloud Security Service zawiera funkcję zarządzania kluczami, która obsługuje klucze kryptograficzne (statyczne lub generowane dynamicznie) niezbędne przy komunikacji pomiędzy różnymi komponentami. Przy użyciu odpowiedniej technologii kluczy, łącznik zapewnia bezpieczną komunikację i dba o to, aby cały ruch był przenoszony prawidłowo i bezpiecznie przez wiele protokołów proxy.

Bezpieczny, niewielkich rozmiarów łącznik znajduje się w centrum danych i jest przyjazny dla zapory, gdyż używa standardowych portów i protokołów dla całej komunikacji pomiędzy przedsiębiorstwem a zasobami cloud. Większość przedsiębiorstw nie będzie więc musiało wprowadzać żadnych zmian do ustawień zapory. W każdym przypadku podczas komunikacji z zasobami cloud używane są w pełni zakodowane kanały komunikacji.

Cloud Security Broker

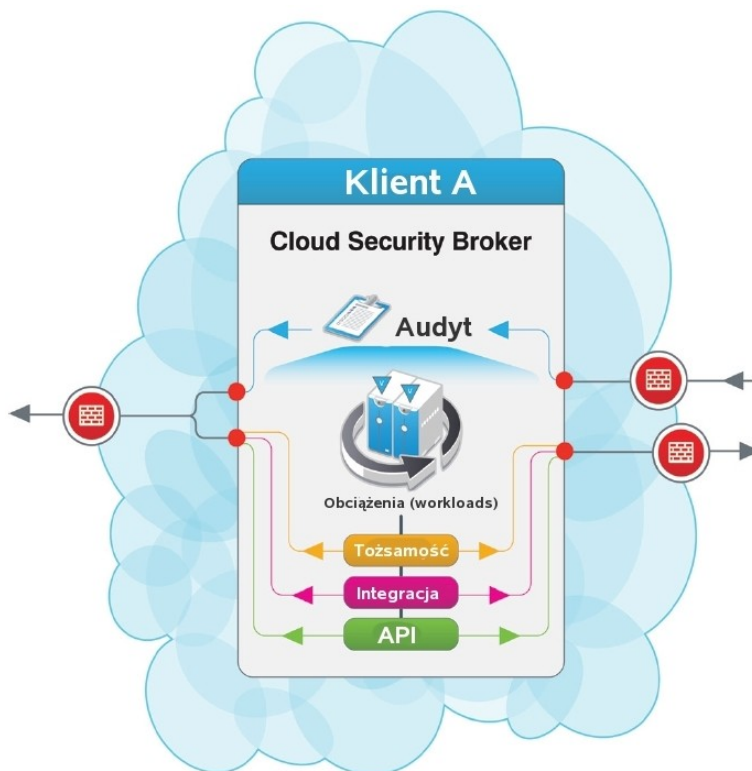
Gdy konektory do dostawcy usług SaaS/PaaS oraz do przedsiębiorstwa są w stanie gotowości, cała praca związana z kontrolą tożsamości i zapewnieniem bezpieczeństwa zostaje przeniesiona do Cloud Security Service, w sercu którego znajduje się Cloud Security Broker.



Ilustracja 4. Cloud Security Broker znajduje się w przestrzeni cloud.

Cloud Security Broker jest umiejscowiony w przestrzeni cloud, która zazwyczaj znajduje się w miejscu, gdzie dostawca SaaS przechowuje swoją aplikację. Może być również przechowywany przez firmę Novell wraz z jednym z partnerów od hostingu lub u któregoś z dostawców usług IaaS (*Infrastructure as a Service*). Cloud Security Broker jest obsługiwany przez takich dostawców IaaS jak Amazon EC2, GoGrid, XEN, Eucalyptus oraz dowolną usługę IaaS wykorzystującą VMware ESX. Cloud Security Broker obsługuje bezpieczny łącznik, który komunikuje się z przedsiębiorstwem i utrzymuje połączenie z każdym konektorem usług SaaS lub PaaS.

Cloud Security Broker jest zbiorem elementów przestrzeni cloud działających razem w celu zapewnienia bezpiecznej przestrzeni dla obciążeń cloud i danych przechowywanych w środowisku cloud. Ilustracja 5 pokazuje schemat modułu Cloud Security Broker. W centrum diagramu znajdują się chronione obciążenia. Obciążenie to dowolna usługa działająca na komputerze, np. serwer sieci Web, serwer poczty email lub systemy ERP, np. SAP. Obciążenia te mogą być przypisane do przedsiębiorstwa (jak w przypadku obciążeń przenoszonych z centrum danych do przestrzeni cloud), jak również mogą być procesami pomocniczymi wymaganymi przez Cloud Security Broker.



Ilustracja 5. Cloud Security Broker

Obciążenia te mogą łączyć się z zasobami przedsiębiorstwa przez integrację tradycyjnych protokołów lub za pomocą interfejsu API dla oprogramowania Cloud Security Broker. Integracja tradycyjnych protokołów nawiązuje do powszechnych sposobów komunikacji pomiędzy sieciami poprzez wykorzystanie protokołów HTTP, HTTPS oraz LDAP. Na przykład typowe obciążenie (korzystające z LDAP do pozyskiwania określonych atrybutów tożsamości oraz dokonania uwierzytelnienia) może działać dalej bez żadnej modyfikacji za pomocą oprogramowania Cloud Security Broker oraz przy użyciu proxy LDAP. Proxy LDAP współdziała z elementami spoza brokera przy pomocy bezpiecznego łącznika. W innym przypadku obciążenie może uzyskiwać dostęp do atrybutów tożsamości lub dokonywać uwierzytelniania poprzez platformę/API dla oprogramowania Cloud Security Broker, co zdecydowanie zwiększa funkcjonalność rozwiązania. Integracja tradycyjnych protokołów umożliwia również integrację tożsamości oraz integrację rozwiązań GRC (Governance, Risk i Compliance), co jest potrzebne do zapewnienia odpowiedniej funkcjonalności obsługi tożsamości, przeprowadzania audytu i zapewniania zgodności z przepisami. W przypadku dostępu do tożsamości (gdy korzysta się z platformy/API oprogramowania Cloud Security Broker) integracja tożsamości i integracja GRC zostają znacznie usprawnione.

Novell Cloud Security Service zapewnia bezpieczną inkorporację zasobów cloud, gdyż dostęp do nich może odbywać się za pomocą rozwiązania Cloud Security Broker lub z poziomu konektorów znajdujących się w środowiskach SaaS lub PaaS. Bezpieczna inkorporacja możliwa jest dzięki interakcji pomiędzy obciążeniami, platformą/API, rozwiązaniami do integracji tradycyjnych protokołów, integracji tożsamości oraz integracji GRC. Równolegle mamy bezpieczny dostęp do zasobów przy pomocy bezpiecznego łącznika. Ponadto bezpieczeństwo zostaje zwiększone poprzez użycie kluczy kryptograficznych przechowywanych w centrum danych przedsiębiorstwa lub lokalnych środowiskach i wysłanych do rozwiązania Cloud Security Broker poprzez bezpieczny łącznik.

Zalety modelu inkorporacji bezpieczeństwa

Inkorporacja obejmuje następujące zagadnienia biznesowe:

- **Ochrona tożsamości.** Inni dostawcy tożsamości w przestrzeni cloud synchronizują informacje o tożsamości (lub dane uwierzytelniające z tokenów) pomiędzy przedsiębiorstwem i środowiskiem cloud lub też wykorzystują technologię proxy do jednokrotnej autoryzacji (single sign-on) poprzez użycie mechanizmów wypełniania formularzy. Tymczasem Novell Cloud Security Service oprócz ww. funkcjonalności umożliwia znacznie więcej. Usługi stają się bezpieczne w przestrzeni cloud, gdyż dane uwierzytelniające nigdy nie zostają ujawnione, tylko stanowią podstawę dla list uwierzytelniających do ochrony obecności przedsiębiorstwa w przestrzeni cloud.
- **Raportowanie zgodności z regulacjami.** Inkorporacja zasobów przestrzeni cloud byłaby niekompletna, gdyby zakończona została na poziomie samej kontroli tożsamości. Reguły biznesowe muszą zostać przekazane do przestrzeni cloud oraz muszą być przestrzegane. Novell Cloud Security Service umożliwia przekazywanie informacji o zdarzeniach dotyczących zgodności z przepisami z przestrzeni cloud do centrum danych, wyszczególniając fakt użycia tożsamości, danych i procesów w przestrzeni cloud oraz działań użytkowników w tejże przestrzeni. Innymi słowy, przedsiębiorstwo bezpiecznie korzysta z przestrzeni cloud.
- **Ochrona przechowywanych informacji.** Problem dostępu do danych przechowywanych w przestrzeni cloud będzie stawał się coraz bardziej istotny w miarę rozwoju rozwiązań cloud. Novell jest jedynym dostawcą oferującym zintegrowany i bezpieczny dostęp do usług przechowywania w przestrzeni cloud. Jeżeli zezwoli na to dostawca usług SaaS, Cloud Security Service udostępnia oparte na kluczach szyfrowanie miejsc przechowywania danych w przestrzeni cloud. Klucz jest przechowywany pod osłoną zapory przedsiębiorstwa i bezpiecznie przenoszony przez Internet do miejsc przechowywania zasobów w przestrzeni cloud, dzięki czemu szyfrowanie i odszyfrowywanie będzie zachodziło bez ujawniania klucza i narażania się na działania hakerów. Novell Cloud Security Service monitoruje również miejsce przechowywania danych w przestrzeni cloud, aby zapewnić zgodność z mającymi zastosowanie regulacjami prawnymi.
- **Rozszerzenia do procesu obiegu zadań (workflow).** Koncepcja inkorporacji pozwala na przeniesienie obiegu pracy poza tradycyjną granicę przedsiębiorstwa, umożliwiając zarządzanie zasobami przestrzeni cloud na zasadach biznesowych tego przedsiębiorstwa.

Wnioski

Sukces rozwiązań opartych na cloud computing zależy od tego, czy przestaną one reprezentować odrębne i odmienne środowiska operacyjne. Z punktu widzenia firmy dodanie nowego środowiska operacyjnego i tym samym problemów dotyczących polityk i zgodności z przepisami w tym środowisku, oznacza zwiększenie stopnia skomplikowania IT, a w konsekwencji możliwość zakłóceń w pracy oraz kłopoty z zarządzaniem. Sposobem na uniknięcie tych problemów oraz na zapewnienie udanego wejścia w rozwiązania cloud computing i przechowywania danych w przestrzeni cloud jest uczynienie przestrzeni cloud naturalnym przedłużeniem posiadanego centrum danych. To właśnie jest zadanie dla Novell Cloud Security Service. Novell posługuje się procesem zwanym „inkorporacją” w celu rozciągnięcia posiadanej w firmie infrastruktury i miejsca do przechowywania informacji na przestrzeń cloud. Novell jednocześnie gwarantuje, że polityki biznesowe oraz praktyki operacyjne przedsiębiorstwa mogą być jednakowo egzekwowane zarówno w przestrzeni cloud, jak i w posiadanym centrum danych. Inkorporacja czyni usługi typu cloud bezpiecznymi dla przedsiębiorstw dzięki temu, że poufne dane są zawsze chronione znajdując się za firmową zaporą.

Cloud Security Service zapewnia dostawcom rozwiązań cloud wiele korzyści oferując wbudowaną integrację z systemami przechowującymi informacje o tożsamości, gotowe systemy raportowania zgodności z przepisami oraz przyjazne dla użytkowników mechanizmy jednokrotnej autoryzacji. Cloud Security Service daje dostawcom rozwiązań cloud konkurencyjną przewagę, wnosząc ponad 20 lat doświadczenia firmy Novell w rozwoju wiodących na rynku produktów do obsługi tożsamości, kontroli

dostępu oraz zapewnienia bezpieczeństwa. Ponadto samo rozwiązanie Novell Cloud Security Service jest również udostępniane w modelu cloud i oferuje usługę pay-as-you-go, która umożliwia redukcję kosztów ogólnych związanych z operacjami biznesowymi, zarówno u dostawców rozwiązań cloud, jak i w samych przedsiębiorstwach.

Więcej informacji

Szczegółowe informacje o oprogramowaniu firmy Novell dla środowiska typu cloud można znaleźć na stronie: www.novell.com/cloud.

Novell Sp. z o.o.
ul. Postępu 21
02-676 Warszawa
tel. 0 22 537 5000
bezpłatna infolinia 0 800 22 66 85
infolinia@novell.pl

462-PL2138-001 | 10/09 | © 2009 Novell Inc. Wszelkie prawa zastrzeżone. Novell, logo Novell i logo N są zastrzeżonymi znakami towarowymi firmy Novell Inc. w Stanach Zjednoczonych i innych krajach.

* Pozostałe znaki towarowe są własnością odpowiednich podmiotów.