

Novell Access Manager 3

Kontrola dostępu, zarządzanie regułami, zapewnienie zgodności

Wprowadzenie

Konkurencyjność współczesnej firmy wymaga, by jej mechanizmy biznesowe były dostępne dla pracowników, klientów i partnerów niezależnie od miejsca i pory dnia. Oprogramowanie Novell® Access Manager stanowi odpowiedź na to wyzwanie, zapewniając maksymalną dostępność dla użytkowników bez zmniejszania poziomu bezpieczeństwa i kontroli. Rozwiązanie wykorzystuje opracowane przez Novella mechanizmy bezpieczeństwa, co pozwala ograniczyć ryzyko i zwiększyć elastyczność kontaktów z klientami, partnerami i kontrahentami.

Novell Access Manager 3 pozwala wzmocnić zaufanie w kontaktach biznesowych. Produkt ten upraszcza i zabezpiecza współużytkowanie zasobów online, udostępniając nową metodę kontrolowania dostępu do aplikacji biznesowych, i to zarówno tradycyjnych, jak i internetowych. Zaufani użytkownicy są bezpiecznie uwierzytelniani i uzyskują dostęp do portali, treści WWW i aplikacji korporacyjnych, natomiast administratorzy systemów informatycznych mają możliwość opartego na regułach zarządzania uwierzytelnianiem i prawami dostępu do środowisk WWW i aplikacji korporacyjnych. Co więcej, oprogramowanie Novell Access Manager obsługuje szeroki zakres platform i usług katalogowych i jest dostatecznie elastyczne, by pracować nawet w najbardziej złożonych heterogenicznych środowiskach informatycznych. Użytkownicy szczególnie cenią możliwość kontroli dostępu do aplikacji Java uruchamianych w środowiskach IBM WebSphere, BEA WebLogic i JBOSS.

Definiowanie praw dostępu oparte na tożsamości

Novell Access Manager to rozwiązanie nowej generacji do zarządzania dostępem i obsługi federacji tożsamości. Przedsiębiorstwa (przez co dalej będziemy rozumieć również instytucje) używają produktu Novell Access Manager do kontrolowania dostępu użytkowników wewnętrznych i zewnętrznych do zawartości sieci, aplikacji oraz usług. Kluczowe komponenty oprogramowania Novell Access Manager — służące do zarządzania tożsamością i obsługi federacji — są oparte na czołowych standardach branżowych, takich jak Liberty Alliance, Web Services Security (WS-Security) i Security Assertion Markup Language (SAML — język znakowania potwierdzeń bezpieczeństwa).

Dział IT firmy może korzystać z narzędzi umożliwiających bezpieczne i proste definiowanie praw dostępu do aplikacji internetowych i udostępnianych na serwerach korporacyjnych. Zasoby są udostępniane na podstawie roli użytkownika w firmie lub jego powiązania z firmą.

Standardowe mechanizmy jednokrotnego logowania

Hasła mogą sprawiać kłopot, ale nie tylko użytkownikom ze względu na swe istnienie, lecz przez ich „umieszczenie” — np. na karteczkach przyklejonych na monitorach, klawiaturach i w innych oczywistych miejscach w biurze. Oznacza to, że hasła mogą stanowić poważne zagrożenie dla bezpieczeństwa, zwłaszcza gdy wykonywanie codziennych obowiązków wymaga od użytkowników używania kilku różnych haseł. Dlatego oprogramowanie Novell Access Manager obsługuje jednokrotne logowanie, dzięki czemu każdy pracownik czy partner musi znać tylko jedno hasło, by uzyskać autoryzowany dostęp do wszystkich przyznanych mu korporacyjnych aplikacji internetowych.

Uproszczone federowanie tożsamości

Novell Access Manager daje możliwość federowania aplikacji bez konieczności modyfikacji treści ani instalowania dodatkowego oprogramowania na serwerze WWW. Dzięki temu tożsamości użytkowników można natychmiast sfederować, i to po obu stronach zapory sieciowej.

Uproszczone, scentralizowane administrowanie

Novell Access Manager ułatwia administrowanie, umożliwiając scentralizowanie kontroli dostępu do wszystkich zasobów elektronicznych i eliminując konieczność korzystania z różnych narzędzi dla różnych lokalizacji. Centralne rozwiązanie kontroli dostępu obsługuje wszystkie aplikacje i zasoby informacyjne. Co więcej, Novell Access Manager obsługuje najważniejsze standardy federacji, w tym SAML i Liberty Alliance.

Zgodność z przepisami

Novell Access Manager daje możliwość generowania raportów zawierających szczegółowe informacje o dowolnym zdarzeniu w sieci, pokazując na przykład, kto i kiedy uzyskał dostęp do wybranego zasobu. Dzięki temu łatwo jest kontrolować zgodność z przepisami. Czy to w przypadku oceny wewnętrznej, czy audytu zewnętrznego, Novell Access Manager udostępnia raporty wymagane dla utrzymania zgodności z wymaganiami Sarbanes-Oxley, HIPAA, Unii Europejskiej i innymi przepisami prawnymi.

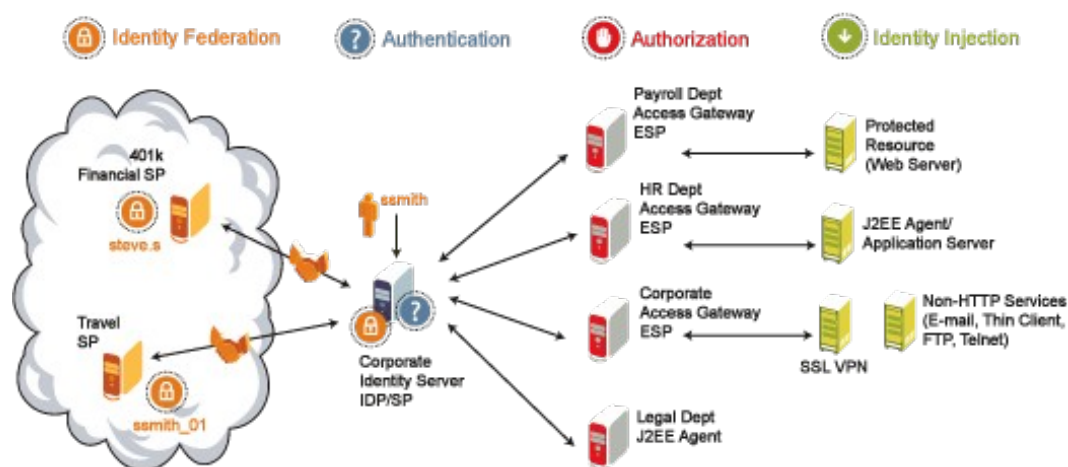
Korzyści i powody stosowania produktu Novella

Novell Access Manager pozwala:

- Udostępniać niezbędne zasoby informatyczne użytkownikom znajdującym się poza firmową zaporą sieciową
- Współdzielić informacje o tożsamości i prawach dostępu z zaufanymi partnerami
- Nadawać i usuwać prawa dostępu w czasie rzeczywistym
- Sprawdzać zgodność działalności firmy z przepisami w czasie rzeczywistym
- Generować raporty dotyczące zdarzeń w sieci i prób dostępu.

Jak działa Novell Access Manager

Novell Access Manager jest idealnym rozwiązaniem dla firm wymagających autoryzacji dostępu do usług udostępnianych przez HTTP i/lub innymi drogami. Podstawowym zastosowaniem oprogramowania Access Manager w tym zakresie jest zarządzanie dostępem (uwierzytelnianie i autoryzowanie użytkowników) oraz federowanie tożsamości. Rysunek 1 ilustruje metody integrowania komponentów produktu Access Manager w celu osiągnięcia wymienionych celów.



Rys. 1. Metody integrowania komponentów produktu Access Manager

Większość wdrożeń oprogramowania Access Manager wykorzystuje serwery tożsamości i bramy dostępowe w celu zapewnienia kontroli dostępu opartej na regułach. Instalowanie i konfigurowanie

komponentów SSL VPN i agenta J2EE jest wymagane jedynie w przypadku konieczności ochrony aplikacji niekorzystających z protokołu HTTP i aplikacji Java.

Uwierzytelnianie

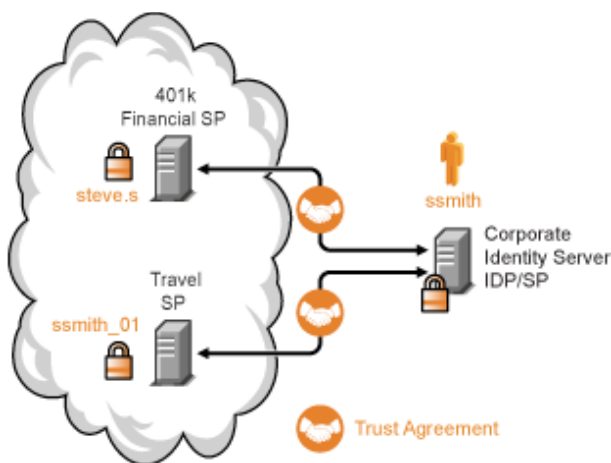
Podstawowym przeznaczeniem serwera tożsamości jest uwierzytelnianie lokalne. Uwierzytelnienie takie jest następnie w imieniu użytkownika udostępniane innym dostawcom (poświadczane). Access Manager obsługuje szereg metod uwierzytelnienia pozwalających zapobiegać nieautoryzowanemu dostępowi, w tym uwierzytelnianie za pomocą hasła, żetonów RADIUS i certyfikatów cyfrowych X.509. Metody uwierzytelnienia są definiowane w kontraktach udostępnianych innym komponentom produktu Access Manager, jak na przykład brama dostępu.

Dane użytkowników są składowane w repozytoriach. Repozytoria użytkowników to serwery katalogowe LDAP, w których użytkownicy się uwierzytelniają. Każde repozytorium może istnieć w kilku kopiach, co pozwala korzystać z możliwości wyrównywania obciążenia i przełączania awaryjnego.

Federowanie tożsamości

Podczas uwierzytelniania użytkownika na żądanie dostawcy usługi istnieje opcja sfederowania tożsamości użytkownika z kontem tego użytkownika u wybranego dostawcy tożsamości. Spowoduje to utworzenie powiązania konta danego użytkownika u dostawcy tożsamości i u dostawcy usługi, a tym samym daje możliwość jednokrotnego logowania i wylogowania.

Jak widać na rys. 2, pewien pracownik o imieniu Steve ma w swojej firmie (u korporacyjnego dostawcy tożsamości) konto o nazwie ssmith. Ma on również osobne konta u poszczególnych dostawców usługi wymaganych do pracy, którzy wspólnie tworzą krąg zaufania.



Rys. 2. Federowanie tożsamości

W tym przykładzie dwaj dostawcy usług są konfigurowani tak, by ufać tożsamości przedstawianej przez korporacyjnego dostawcę tożsamości. Konta Steve'a u poszczególnych dostawców usług mogą zatem zostać powiązane z jego kontem u korporacyjnego dostawcy tożsamości.

Z punktu widzenia administrowania, tego typu współużytkowanie informacji pozwala ograniczyć koszty zarządzania tożsamością, gdyż nie ma potrzeby zbierania i składowania danych związanych z tożsamością (na przykład haseł) przez każdą organizację z osobna. Rozwiązanie to zapewnia też bardziej komfortową pracę użytkownikowi dzięki zmniejszeniu liczby operacji logowania. Należy zwrócić

uwagę, że to użytkownik kontroluje federację tożsamości swoich kont, czyli odpowiada za federowanie (łączenie) i defederowanie swoich danych identyfikacyjnych.

W wewnętrznych środowiskach firmowych federowaniem danych o tożsamości użytkowników zajmują się na ogół administratorzy, postępując zgodnie z przyjętymi regułami dotyczącymi ról pełnionych przez użytkowników w organizacji.

Autoryzacja

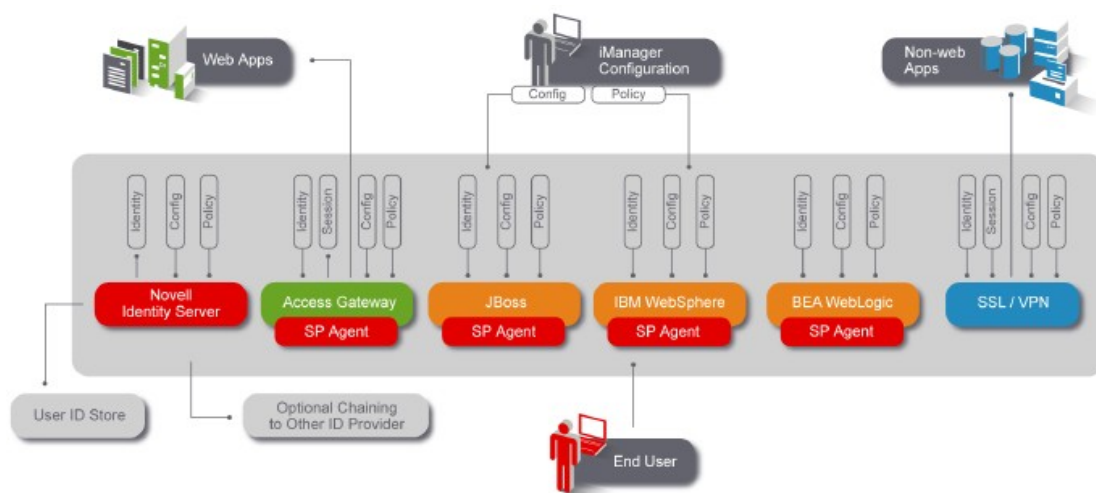
Reguły autoryzacji są używane, gdy potrzebna jest kontrola dostępu do zasobu według innych kryteriów niż samo uwierzytelnienie i ma ją przeprowadzać produkt Access Manager. Reguły autoryzacji są stosowane po zalogowaniu użytkownika i nawiązaniu połączenia, w chwili zażądania przez użytkownika danych z chronionego zasobu.

Wstawianie tożsamości

Technika wstawiania tożsamości pozwala dodawać określone dane do adresu URL lub strony HTML przed wysłaniem na serwer WWW. Serwer wykorzystuje te informacje do ustalenia, czy użytkownik powinien uzyskać dostęp do zasobu. Serwer WWW określa też, jakie informacje należy wstawić, by umożliwić dostęp do zasobu.

Komponenty produktu Novell Access Manager

Pełna integracja komponentów oprogramowania Novell Access Manager zapewnia kontrolę dostępu na wszystkich poziomach. Komponenty te są przedstawione na rys. 3.



Rys. 3. Komponenty oprogramowania Novell Access Manager

Komponenty produktu Novell Access Manager są przedstawione na ilustracji w środku. Kilka magazynów identyfikatorów użytkowników może zostać zagregowanych za pośrednictwem jednego serwera tożsamości (Identity Server). Można tu użyć dowolnej kombinacji następujących usług katalogowych:

- Novell eDirectory™
- Sun ONE Directory Server
- Microsoft Active Directory.

W dalszych podrozdziałach podane są bardziej szczegółowe informacje dotyczące komponentów oprogramowania Novell Access Manager oraz jego możliwości funkcjonalnych.

Zarządzanie regułami w produkcie Novell Access Manager

Podstawowe możliwości oprogramowania Novell Access Manager to zarządzanie regułami (*policy*) i egzekwowanie reguł. Wszystkie jego komponenty są sterowane regułami definiowanymi przez użytkowników. Reguły te są rutynowo egzekwowane i rejestrowane dla potrzeb raportowania zgodności z przepisami.

Serwer tożsamości

Serwer tożsamości (*Identity Server*) zapewnia usługi uwierzytelniania na rzecz wszystkich komponentów oprogramowania Novell Access Manager. Ponadto udostępnia usługi dostawcy (*provider*) i konsumenta (*consumer*) dla potrzeb żądań w standardach Liberty Alliance i SAML (wersja 1.1 i 2.0). Podobnie jak w przypadku wszystkich komponentów oprogramowania Novell Access Manager, serwer tożsamości zapewnia usługi uwierzytelniania zgodne z deklaracjami reguł menedżera tożsamości.

Serwer tożsamości uwierzytelnia użytkowników oraz dostarcza informacji o ich rolach, co umożliwia podejmowanie decyzji o autoryzacji lub odmowie udzielenia dostępu. Ponadto zawiera pełną platformę usług internetowych Liberty Alliance Web Service Framework, która może być użyta do dystrybuowania informacji o tożsamości. Przedsiębiorstwa mogą używać udostępnianych przez serwer tożsamości profili (pracownika, osoby), zgodnych ze standardem Liberty Alliance, ewentualnie definiować atrybuty niestandardowe i używać ich przy egzekwowaniu reguł.

Serwer tożsamości ułatwia również obsługę federacji (*federated provisioning*), zapewniając automatyczne tworzenie kont użytkowników w wyniku żądania federacji. Gdyby nie było takiej możliwości, użytkownicy musieliby się zarejestrować (założyć konto użytkownika) u usługodawcy przed sfederowaniem tożsamości.

Brama dostępu

Brama dostępu (*Access Gateway*) to komponent oprogramowania Novell Access Manager udostępniający usługi proxy HTTP. Udostępnia ona znakomite usługi ochrony i proxy (obejmujące autoryzację, jednokrotne zalogowanie oraz szyfrowanie danych), a ponadto jest zintegrowana z nowymi usługami produktu Novell Access Manager związanymi z tożsamością i regułami.

Brama dostępu umożliwia przedsiębiorstwom przekształcenie uwierzytelniania realizowanego przez dostawcę tożsamości (*Identity Provider*) i innych usług takiego dostawcy w standardowe nagłówki WWW, odpowiedzi oparte na wypełnieniu formularza oraz podstawowe odpowiedzi uwierzytelniające. Inaczej mówiąc, brama dostępu umożliwia przedsiębiorstwu wykorzystanie istniejących aplikacji internetowych — bez jakiegokolwiek ich modyfikacji — i realizację uwierzytelniania do nich kontrolowanego za pomocą reguł Novell Access Management.

Na przykład brama dostępu zawiera funkcję „wstawiania tożsamości” (*Identity Injection*) w oparciu o reguły. Umożliwia ona wykorzystanie platformy Liberty Alliance Web Service Framework do wydobywania informacji o tożsamości oraz następnie wstawienia ich do nagłówków WWW lub ciągów znaków zawierających zapytania.

Agenty serwera aplikacji Javy

Do wyboru są trzy agenty serwera aplikacji Javy: IBM WebSphere, BEA WebLogic i JBoss. Agenty te wykorzystują usługi Java Authentication and Authorization Service (JAAS — usługa uwierzytelniania i autoryzacji na platformie Java) i Java Authorization Contract for Containers (JACC — kontrakt autoryzacji dla kontenerów na platformie Java) oraz wewnętrzne interfejsy programowe (API) serwera WWW do uwierzytelniania, a także zapewniają dostęp do obiektów Java Servlet i Enterprise JavaBeans kontrolowany w oparciu o reguły. W niektórych przypadkach przedsiębiorstwa mogą uzyskać ściślejszą i solidniejszą integrację dzięki użyciu interfejsów API specyficznych dla danej platformy.

SP Agent

SP Agent to współużytkowany komponent, który udostępnia wspólną implementację standardów i protokołów związanych z tożsamością i federacją. Agent ten przekierowuje wszystkie żądania uwierzytelnienia do serwera tożsamości, który z kolei zwraca do komponentu potwierdzenie (*assertion*) SAML. Obecność potwierdzeń SAML w każdym komponencie menedżera dostępu pozwala chronić poufną informację, w tym w szczególności eliminuje potrzebę przekazywania upoważnień użytkownika pomiędzy komponentami w celu zarządzania sesją.

SP Agent umożliwia komponentom użycie dostawcy tożsamości do uwierzytelniania i świadczenia usług. Umożliwia także dostawcy tożsamości połączenie łańcuchowe z innymi dostawcami tożsamości. Proces ten, określany jako IDP proxying, ułatwia przedsiębiorstwom tworzenie grup powiązanych ze sobą dostawców tożsamości. W terminologii Liberty Alliance takie grupy są określane jako „kręgi zaufania” (*Circles of Trust*).

SSL VPN

SSL VPN zapewnia bezpieczny dostęp do aplikacji nieopartych na HTTP. Jest to usługa linuksowa, zaś brama dostępu z jednej strony przyspiesza jej działanie, a z drugiej strony współużytkuje wraz z nią informację o sesji.

Gdy użytkownik uwierzytelnia się pomyślnie za pomocą SSL VPN, do klienta zostaje dostarczona wstawka (*plug-in*) ActiveX lub aplet Javy. Funkcja kontroli dostępu w oparciu o role — zapewniana przez Novell Access Manager — determinuje decyzje o autoryzacji dla potrzeb aplikacji zaplecza. Ponadto SSL VPN dokonuje sprawdzenia integralności klienta.

Mechanizm reguł

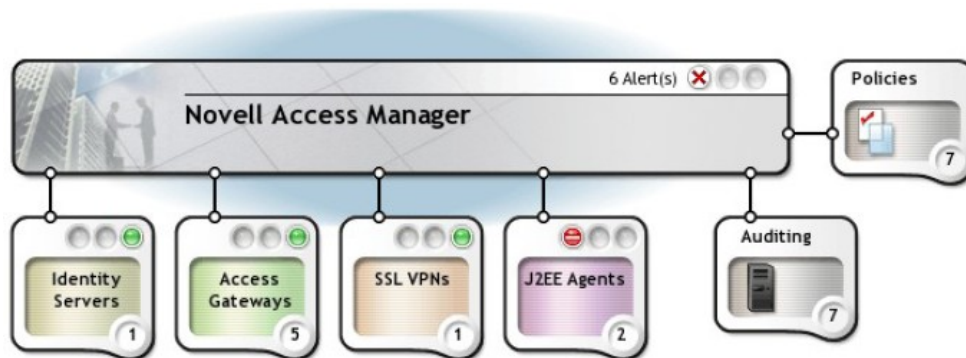
Mechanizm reguł (*Policy Engine*) to komponent oprogramowania Novell Access Manager, który zapewnia rozstrzygnięcie wszystkich reguł dla potrzeb wszystkich pozostałych komponentów produktu. Dla zwiększenia wygody umożliwia on także definiowanie reguł w kategoriach ról użytkowników.

Interfejs zarządzania

Interfejs administracyjny produktu Novell Access Manager stanowi centralne miejsce, z którego konfiguruje się wszystkie komponenty i reguły produktu oraz zarządza nimi. Przedsiębiorstwa mogą także używać tego interfejsu do grupowania różnych bram dostępu w celu wdrażania zmian konfiguracji równocześnie we wszystkich elementach grupy. Istnieje możliwość delegowania uprawnień administracyjnych w odniesieniu do poszczególnych urządzeń, agentów oraz kontroli reguł.

Scenariusze wdrożenia i wykorzystania

W tym rozdziale opisane są różne scenariusze wdrożenia i użycia produktu Novell Access Manager.



Rys. 4. Konsola zarządzania oprogramowania Novell Access Manager

Zarządzanie oprogramowaniem Novell Access Manager

Administratorzy nadzorujący urządzenia, grupy i reguły zarządzane przez Novell Access Manager zwykle mają przypisaną w katalogu rolę administratora urządzeń (*Device Administrator*) lub administratora reguł (*Policy Administrator*).

Rys. 4 przedstawia widok najwyższego poziomu udostępniany przez interfejs administracyjny oprogramowania Novell Access Manager. Na tym najwyższym poziomie wszyscy administratorzy mogą widzieć status wszystkich urządzeń i reguł, a także wszystkie ewentualne ostrzeżenia lub alarmy. Na ilustracji widać m.in., że co najmniej jeden agent J2EE jest w stanie krytycznym (status czerwony, zapalona lewa lampka kontrolna podobna do znaku drogowego „zakaz wjazdu”). Jest tak dlatego, że alarmy dotyczące agentów J2EE zostały oznaczone jako „potwierdzone” (*cleared*), ale nie „rozwiązane” (*resolved*). Status „potwierdzony” jest nadawany przez administratora, natomiast status „rozwiązany” jest osiągnięty w wyniku wyłączenia urządzenia bądź przywrócenia jego pełnej sprawności (status zielony). W określonych sytuacjach może też pojawić się stan żółty (ostrzegawczy).

Przedsiębiorstwa mogą wykorzystywać funkcje administracyjne oprogramowania Novell Access Manager dla potrzeb następujących komponentów i procesów:

- serwery tożsamości
- bramy dostępu (dla produktów działających w systemach Linux, Open Enterprise Server i NetWare)
- sieci VPN SSL
- agenty Javy
- zarządzanie urządzeniami
- zarządzanie regułami.

Każdy panel na rysunku wskazuje łączną liczbę urządzeń w danej kategorii oraz zagregowany status alarmów dla wszystkich urządzeń w tej kategorii. Na przykład serwer tożsamości (w tym przykładzie występuje tylko jeden) jest w stanie w pełni funkcjonalnym. Status ten jest reprezentowany zielonym kółkiem na trzeciej pozycji statusu alarmu na panelu serwerów tożsamości. Podobnie jak widać dostępnych jest pięć bram dostępu. Istnieje także nierozwiązany alarm krytyczny dotyczący co najmniej jednego agenta J2EE, na co wskazuje czerwone kółko na panelu agentów J2EE. Administrator może po prostu kliknąć dany panel, aby wyświetlić nierozwiązane problemy dotyczące urządzeń z kategorii

reprezentowanej przez ten panel. Warto zapamiętać, że chociaż problem może być wyświetlony przez każdego administratora, modyfikacje lub działania korekcyjne mogą być podejmowane tylko przez administratorów, którzy mają uprawnienia dostępu do danego urządzenia lub reguły.

Panel urządzeń wymaga specjalnego wyjaśnienia. Wszystkie komponenty linuksowe mogą być wdrażane na serwerach w sposób mieszany, tzn. na przykład jeden serwer fizyczny może być hostem dla serwera tożsamości oraz dla kilku agentów J2EE. Jeśli dany serwer ulegnie awarii, wszystkie komponenty, dla których ten serwer jest hostem, będą wykazywać odpowiedni status alarmu. W celu umożliwienia administratorom szybkiego skorygowania takiego problemu, alarmy związane z serwerami są wyświetlane oddzielnie w panelu urządzeń.

Jeśli panel urządzeń wykazuje status alarmu (żółty lub czerwony) dla danego serwera, wszystkie komponenty, dla których ten serwer jest hostem, mogą także generować alarmy. Jeśli uprawniony administrator wybierze panel urządzeń, może szybko wyizolować i skorygować problem dotyczący serwera. Skorygowanie problemów na poziomie serwera przypuszczalnie spowoduje także skorygowanie wszystkich problemów dotyczących poszczególnych komponentów.

Panel reguł różni się od pozostałych paneli tym, że nie występuje w nim wskaźnik statusu alarmu. Panel ten umożliwia upoważnionemu administratorowi (posiadającemu uprawnienia dostępu w zakresie sekcji zarządzania regułami w interfejsie administracyjnym) tworzenie i edytowanie reguł przypisanych do poszczególnych komponentów, a także zarządzanie takimi regułami. Sekcja administrowania regułami wprowadza dodatkową warstwę kontroli dostępu administratorów. Reguły mogą być podzielone na grupy, zaś administratorzy reguł mogą być przypisani do wybranego podzbioru takich grup reguł. Dzięki temu można dzielić obowiązki pomiędzy poszczególnych administratorów reguł, a także łatwiej rozwiązywać szereg problemów związanych ze zgodnością z przepisami.

Wszystkie uprawnienia dostępu są udzielane administratorom urządzeń i administratorom reguł przez jednego lub więcej administratorów interfejsu administracyjnego oprogramowania Novell Access Manager. Administratorzy ci są upoważnieni tylko do udzielania uprawnień związanych z kontrolą dostępu. Opcjonalnie administratorzy mogą mieć globalne uprawnienia administracyjne, co w praktyce oznacza utworzenie grupy superadministratorów.

Należy zwrócić uwagę na jeszcze jedną dodatkową funkcję. W polu listy rozwijanej można wybrać opcję All Access Sites (Wszystkie ośrodki dostępu). Opcja ta powoduje wyświetlenie wszystkich urządzeń i reguł skonfigurowanych w systemie Novell Access Manager. Inne ośrodki mogą być skonfigurowane przez administratorów w celu wygodnego pogrupowania pewnych podzbiorów urządzeń. Takie ośrodki są tylko logiczne i mogą zawierać usługi należące do innych ośrodków. Na przykład można utworzyć ośrodek „Mazowieckie”, który będzie zawierać usługi i urządzenia zawarte również w ośrodku „Warszawa”.

Podsumowując: Novell Access Manager umożliwia administratorom spełnienie wymagań dotyczących rozdziału obowiązków, co z kolei ułatwia przedsiębiorstwu zapewnienie zgodności z przepisami. Należy podkreślić, że chociaż każdy administrator może zobaczyć każdy status alarmu, modyfikować dane urządzenie mogą tylko ci administratorzy, którzy mają odpowiednie uprawnienia dostępu.

Administrowanie regułami w oprogramowaniu Novell Access Manager

Dostępność funkcji administrowania regułami w skali całego systemu jest bardzo ważną zaletą, która często sama w sobie stanowi uzasadnienie wdrożenia produktu Novell Access Manager. Funkcja administrowania regułami jest zintegrowana z interfejsem zarządzania w taki sposób, że umożliwia rozdzielenie obowiązków pomiędzy administratorów reguł.

Reguły są oparte na punktach egzekwowania reguł (PEP — *Policy Enforcement Point*). Dla każdego komponentu oprogramowania Novell Access Manager jest zdefiniowanych kilka takich punktów PEP. W celu utworzenia reguły, administrator deklaruje najpierw, który punkt PEP będzie kontrolowany przy użyciu danej reguły. Takie wstępne zadeklarowanie daje kilka zalet:

- opcje konfiguracji reguł wyświetlają tylko te wartości i funkcje, które są dostępne dla danego punktu PEP
- przydzielanie reguły do urządzenia może być poddane audytowi, tak aby przy wdrożeniu danej reguły mogły być wybrane tylko odpowiednie urządzenia z kompatybilnymi punktami PEP
- niektóre wartości reguł mogą być obowiązkowe w przypadku jednych reguł, zaś opcjonalne w przypadku innych, jednak pole zawierające taką wartość pozostaje w każdym przypadku to samo, dzięki czemu utrzymanie mechanizmu reguł wymaga kontroli tylko jednego elementu.

Administrowanie regułami umożliwia także przydzielanie reguł do różnych komponentów menedżera dostępu. Taki przydział obowiązuje tak długo, jak długo dany komponent obsługuje punkt PEP, na którym może działać dana reguła. Administrator ma do dyspozycji narzędzia pozwalające na sprawdzenie, które reguły są używane, które urządzenia ich używają oraz jakie mogą być konsekwencje ewentualnych zmian dla wdrożenia menedżera dostępu.

W celu ułatwienia raportowania zgodności z przepisami, reguły są podzielone na grupy, które podlegają kontroli dostępu sprawowanej przez różnych administratorów reguł. Dzięki temu możliwe jest skonfigurowanie rozdzielenie obowiązków pomiędzy pracowników odpowiedzialnych za utrzymywanie reguł. Tak więc na przykład administrator o kwalifikacjach odpowiednich do opracowywania i utrzymywania reguł dla bramy dostępu lub dla agenta może nie mieć uprawnień do tworzenia i utrzymywania reguły dla serwera tożsamości.

Novell Access Manager rejestruje wszystkie czynności związane z regułami i generuje raporty dotyczące zgodności z przepisami. W dzienniku kontroli narzędzia odpowiedzialnego za audyt (*Novell Audit*) rejestrowane są na przykład takie czynności, jak tworzenie, modyfikowanie, wyłączenie, ostateczne usuwanie, przydzielanie i użycie reguł. Informacje z dziennika mogą być wyszukiwane przy użyciu zapytań, co pozwala na przykład na określenie, jaka reguła rządziła dostępem w dowolnym momencie w trakcie istnienia reguły. Ponieważ zapisy w dzienniku kontroli w Novell Audit są opatrywane podpisami cyfrowymi oraz łączone w łańcuchy, przedsiębiorstwo może mieć pewność, że dane dotyczące zgodności są dokładne.

Konfigurowanie federacyjne w oprogramowaniu Novell Access Manager

Niektóre tradycyjne systemy wymagają, aby przedsiębiorstwo przechowywało wszystkie informacje dotyczące tożsamości w określonym katalogu i określonym formacie. Wszyscy użytkownicy takiego systemu muszą mieć konto w takim katalogu przed umożliwieniem im korzystania z usług udostępnianych przez taki tradycyjny system.

Novell Access Manager umożliwia automatyczne konfigurowanie tego rodzaju kont bez konieczności samodzielnego, ręcznego rejestrowania się przez użytkowników w katalogu tradycyjnego systemu.

Konfigurowanie federacyjne w produkcie Novell Access Manager jest realizowane przez komponent SP Agent lub przez serwer tożsamości. Jeśli dowolny z tych komponentów zostanie skonfigurowany do automatycznego konfigurowania kont użytkowników, weryfikuje najpierw każde żądanie uwierzytelnienia w celu ustalenia, czy katalog tradycyjnego systemu zawiera konto użytkownika. Jeśli katalog już zawiera takie konto, operacja uwierzytelnienia przebiega normalnie. Jeśli natomiast katalog nie zawiera takiego konta, Novell Access Manager wyciąga odpowiednią informację z serwera tożsamości – przy użyciu potwierdzenia (*assertion*) SAML bądź usługi internetowej dostarczającej takiej informacji – i na tej podstawie tworzy konto użytkownika.

Warto zauważyć, że konto w tradycyjnym systemie może używać aliasu (alternatywnego identyfikatora użytkownika) oraz hasła generowanego losowo. Ta informacja jest utrzymywana przez serwer tożsamości i używana za każdym razem, gdy następuje dostęp do tradycyjnego systemu.

Tradycyjne usługi internetowe a integracja

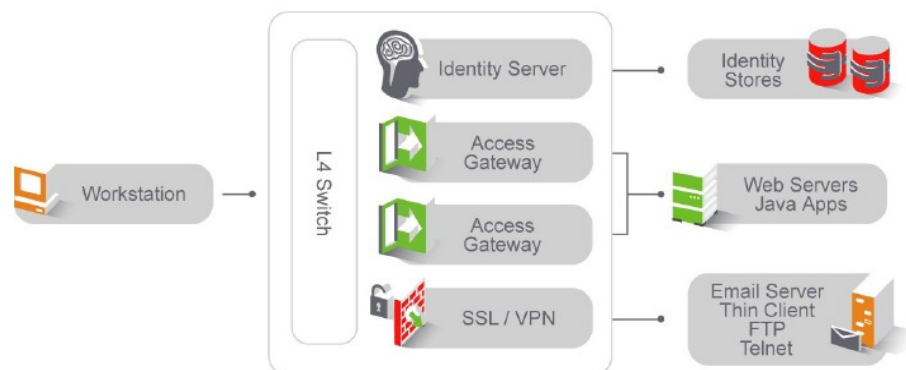
Novell Access Manager umożliwia dostęp do tradycyjnych usług internetowych w wyniku przetworzenia reguł rządzących takimi systemami – przy użyciu takich komponentów, jak agenty J2EE i bramy dostępu. Komponenty te wykonują odpowiednie zadania, jak wypełnianie formularzy, podstawowe uwierzytelnienie i wstawienie nagłówek, niezbędne do zapewnienia użytkownikom bezproblemowego dostępu do tradycyjnych systemów internetowych.

W niektórych przypadkach przedsiębiorstwa wymagają, aby tradycyjne usługi internetowe używały aliasu identyfikatora użytkownika i hasła. Novell Access Manager umożliwia stosowanie dowolnej kombinacji atrybutów z jednego lub więcej magazynów tożsamości w charakterze identyfikatora użytkownika i hasła. Atrybuty te, zawierające odpowiednie identyfikatory użytkownika i hasła, mogą być utrzymywane przez użytkownika bądź przez zautomatyzowany proces. Dzięki temu implementacja mocnych reguł rządzących hasłami może nie kolidować z łatwością użycia.

Ta cecha produktu Novell Access Manager, w połączeniu z funkcją konfigurowania federacyjnego, zapewnia wydajne narzędzie do integracji z tradycyjnymi systemami.

Zarządzanie dostępem do tradycyjnych systemów

Novell Access Manager umożliwia różne metody kontroli dostępu do tradycyjnych systemów:



Rys. 5. Novell Access Manager — schemat ogólny

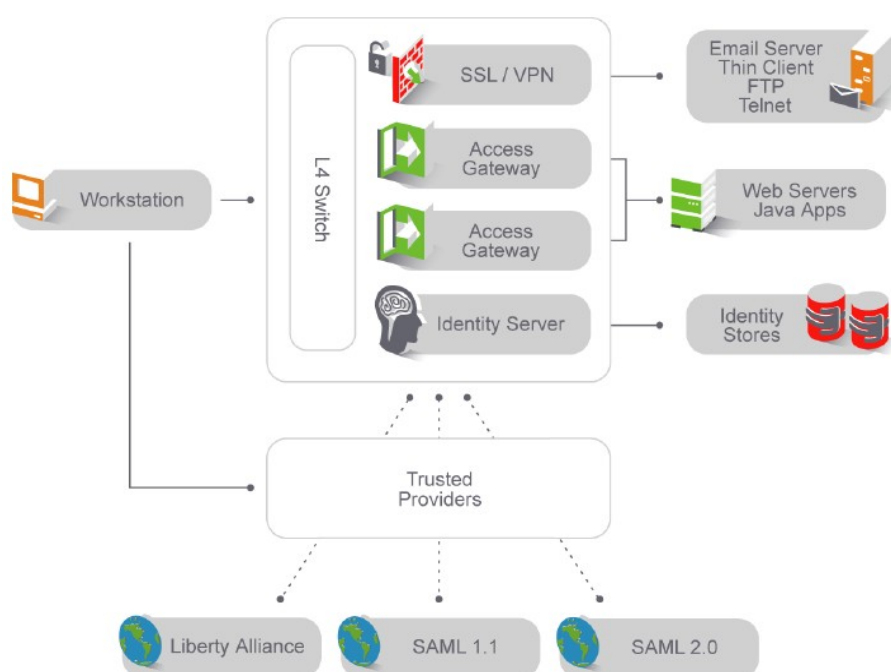
- Serwer tożsamości zapewnia zarządzanie tożsamościami w oparciu o reguły, w tym zarządzanie tożsamościami i/lub rolami sfederowanymi.

- Bramy dostępu zapewniają kontrolę dostępu do zasobów i aplikacji opartych o WWW, przy użyciu tożsamości zarządzanych przez serwer tożsamości. Obejmuje to komponent Novell Access Manager Policy służący do definiowania dostępu do lokalnych zasobów w oparciu o reguły i role.
- Komponent Novell Access Manager Policy umożliwia kontrolę dostępu do zasobów agentów J2EE przez obsługiwane serwery aplikacji.
- SSL VPN zapewnia bezpieczny dostęp w oparciu o tożsamości i role do pozostałych zasobów i aplikacji poza zaporą.

Zarządzanie dostępem a federacja oparta na standardach

Dzięki temu, że Novell Access Manager implementuje specyfikację federacji tożsamości według standardu Liberty Alliance, możliwe jest bezpieczne sfederowanie tożsamości użytkowników.

Podejście do federacji stosowane w produkcie Novell Access Manager uwzględnia przepisy dotyczące zachowania prywatności nawet w przypadku, gdy tożsamości użytkowników są przesyłane za granicę.



Rys. 6. Jednokrotne zalogowanie obejmujące systemy wewnętrzne oraz różne systemy sfederowane lub zaufane

Każde wdrożenie produktu Novell Access Manager obejmuje jeden lub więcej serwerów tożsamości, które koordynują tożsamości użytkowników we wszystkich fazach ich cyklu życia, w tym federację z innymi dostawcami tożsamości kompatybilnymi z Liberty Alliance. Oznacza to, że pomyślne uwierzytelnienie u jednego dostawcy tożsamości kompatybilnego z Liberty Alliance (nawet jeśli nie jest to serwer tożsamości systemu Novell Access Manager) zapewnia uwierzytelnienie również u innych dostawców tożsamości kompatybilnych z Liberty Alliance.

Na przykład pomyślne uwierzytelnienie w serwerze tożsamości systemu Novell Access Manager może być honorowane przez zupełnie oddzielny system, niemający nic wspólnego z systemem Novell Access Manager. Takie uwierzytelnienie może zapewnić użytkownikowi dostęp do zasobów takiego oddzielnego systemu bez konieczności uprzedniego uwierzytelnienia się użytkownika w takim systemie. Ponieważ specyfikacje standardu Liberty Alliance są implementowane po obu stronach, uwierzytelnienie użytkownika może być sfederowane w bezpieczny sposób, z uwzględnieniem wymagań reguł dotyczących prywatności i innych wymogów danego przedsiębiorstwa.

Serwer tożsamości produktu Novell Access Manager jest w pełni zgodny ze specyfikacją standardu Liberty Alliance i obsługuje zarówno wersję SAML 1.1 jak i SAML 2.0. Co więcej, sfederowane tożsamości z systemów zewnętrznych są dostarczane do wszystkich komponentów menedżera dostępu, tak jakby uwierzytelnienie odbyło się w serwerze tożsamości systemu Novell Access Manager. Każda taka sfederowana tożsamość jest przekazywana do obszaru zaufanego (*trust perimeter*) menedżera dostępu zgodnie z regułą lokalną i regułą federacji Liberty Alliance.

Gdy zostanie skonfigurowana umowa federacji z systemami zewnętrznymi, pozostaje ona w mocy zgodnie z regułami wygasania, które są monitorowane i egzekwowane przez Novell Access Manager. W każdym momencie autoryzowany administrator może użyć komponentu administracyjnego produktu Novell Access Manager w celu anulowania, zawieszenia bądź zmodyfikowania umowy federacji.

Odpowiednia reguła może postanawiać, że każda sfederowana tożsamość będzie honorowana w celu umożliwienia jednokrotnego zalogowania się do lokalnych aplikacji tradycyjnych przy użyciu metody jednokrotnego zalogowania za pośrednictwem WWW, wypełniania formularzy, nagłówków HTTP bądź innych metod. Dzięki temu system zarządzania tożsamością udostępnia bogate możliwości funkcjonalne oraz może być w pełni zarządzany zarówno przez przedsiębiorstwo, jak i przez użytkownika.

Zarządzanie dostępem a federacja korporacyjna

Novell Access Manager udostępnia szybszą, uproszczoną metodę uzyskania federacji tożsamości w obrębie przedsiębiorstwa. O ile zewnętrzna federacja tożsamości wymaga interaktywnego dialogu z użytkownikiem w celu określenia reguły federacji, w przypadku „korporacyjnego” trybu federacji Novell Access Manager egzekwuje regułę federacji w oparciu o użytkowników w obrębie całego przedsiębiorstwa.

Ten tryb umożliwia przedsiębiorstwu zdefiniowanie domyślnej reguły federacji, która jest dziedziczona przez użytkowników, gdy ich tożsamości są dodawane do magazynu (magazynów) tożsamości. Każde ustawienie reguły może być oznaczone jako „wymagane” (w takim przypadku nie dopuszcza się modyfikacji przez użytkownika) bądź „opcjonalne” (w takim przypadku dopuszcza się modyfikację przez użytkownika). Po zdefiniowaniu takich instrukcji dla reguły są one egzekwowane automatycznie, bez jakiegokolwiek interakcji z użytkownikiem, i pozostają w mocy tak długo, dopóki nie zostaną zmienione przez przedsiębiorstwo lub użytkownika.

Jeśli tożsamość użytkownika jest sfederowana z serwerem tożsamości lub dostawcą tożsamości zgodnym z Liberty Alliance, ale niedziałającymi w trybie korporacyjnym, to realizowana jest w pełni specyfikacja reguł federacji Liberty Alliance. Tryb korporacyjny systemu Novell Access Manager obejmuje tylko określone, konkretne wdrożenie menedżera dostępu.

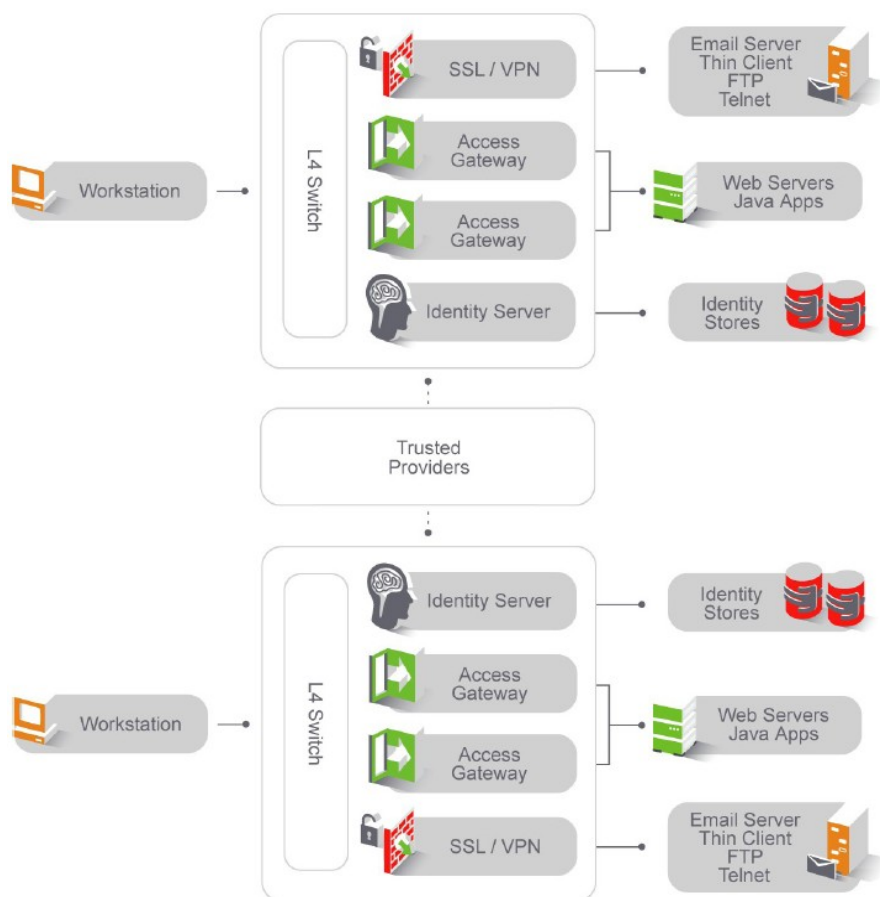
Rejestrowanie dla celów zgodności z przepisami

Novell Access Manager udostępnia ważne funkcje rejestrowania w celu zapewnienia zgodności z przepisami. Każdy komponent tworzy zapisy w dzienniku, odbierane przez narzędzie rejestracji Novell Audit, które pokazują, jak instrukcje reguł wpływają bezpośrednio na decyzje dotyczące dostępu.

Wieloczynnikowa ochrona zasobów

Specyfikacja reguły kontroluje dostęp do wszystkich zasobów chronionych przez program Novell Access Manager. Oznacza to, że uzyskanie dostępu do danego konkretnego zasobu może wymagać spełnienia

więcej niż jednej reguły. Każda reguła może wygenerować inny czynnik kontroli tożsamości niezależnie od specyfikacji pozostałych reguł. Taka możliwość pozwala na uzyskanie wieloczynnikowej ochrony zasobów z bardzo szczegółowym rozróżnianiem na poziomie specyfikacji reguły.



Rys. 5: Przykład federacji korporacyjnej

Najczęściej zadawane pytania (FAQ)

Czy mogę grupowo zarządzać usługami proxy w kilku bramach dostępu pomimo tego, że w każdej z nich jest inny adres IP?

Tak, adresy IP są obsługiwane w taki sposób, że bramy dostępu mogą być zarządzane grupowo.

W jaki sposób moi pracownicy mogą administrować globalnym wdrożeniem systemu Novell Access Manager synchronicznie z upływem czasu lokalnego („podążając za Słońcem”)?

Należy w tym celu przydzielić uprawnienia poszczególnym grupom lub ośrodkom, co pozwoli na nakładanie się obowiązków administracyjnych administratorów niezależnie od położenia geograficznego.

Jestem operatorem Internetu. Czy mogę umożliwić moim klientom pisanie i utrzymywanie ich własnych reguł?

Tak, każdy administrator reguł może mieć uprawnienia ograniczone do konkretnego zbioru instrukcji reguł i zablokowany dostęp poza obrębem tego zbioru.

Czy mogę skonfigurować serwer tożsamości (*Identity Server*) tak, by akceptował on uwierzytelnianie przez proxy?

Tak, serwer tożsamości obsługuje uwierzytelnianie przez proxy.

Czy mogę wdrożyć własnego dostawcę tożsamości (*Identity Provider*) zgodnego z Liberty Alliance?

Tak, serwer tożsamości w pełni obsługuje protokoły Liberty Alliance i może współpracować z innymi instalacjami dostawców tożsamości.

Więcej informacji o oprogramowaniu Novell Access Manager

Szczegółowe informacje o oprogramowaniu Novell Access Manager są dostępne na internetowej stronie produktu pod adresem: www.novell.com/products/accessmanager

INFORMACJE O FIRMIE NOVELL

Novell, Inc. jest dostawcą oprogramowania sieciowego i systemowego, spełniającego kryteria otwartości zgodne z powszechnie uznanymi standardami branżowymi. Posiada przeszło dwudziestoletnie doświadczenie, zatrudnia 5 tys. wysoko kwalifikowanych pracowników, współpracuje z 5 tys. autoryzowanych partnerów i dysponuje globalną siecią centrów wsparcia technicznego. Novell udziela daleko idącej pomocy w zakresie zarządzania, upraszczania, integrowania i zapewniania bezpieczeństwa środowiska informacyjnego przy jednoczesnym obniżaniu kosztów jego posiadania. Novell świadczy usługi dla ponad 50 tys. klientów w 43 krajach, oferując najwyższy, profesjonalny poziom obsługi i dogodne warunki współpracy.

Więcej informacji można uzyskać kontaktując się z bezpłatną Infolinią firmy Novell w Polsce — 0 800 22 66 85, oraz na stronach internetowych www.novell.pl

Copyright © 2006 Novell Inc. Wszelkie prawa zastrzeżone. Novell, logo Novell, logo N, NetWare, SUSE i ZENworks są zastrzeżonymi znakami towarowymi, zaś eDirectory i Sentinel są znakami towarowymi firmy Novell Inc. w Stanach Zjednoczonych oraz innych krajach.

* Linux jest zastrzeżonym znakiem towarowym Linusa Torvaldsa. Pozostałe znaki towarowe należą do odpowiednich właścicieli.