

Novell Access Manager

Kontrola dostępu, zarządzanie regułami, zapewnienie zgodności

Novell.

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 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 potwierżeń 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

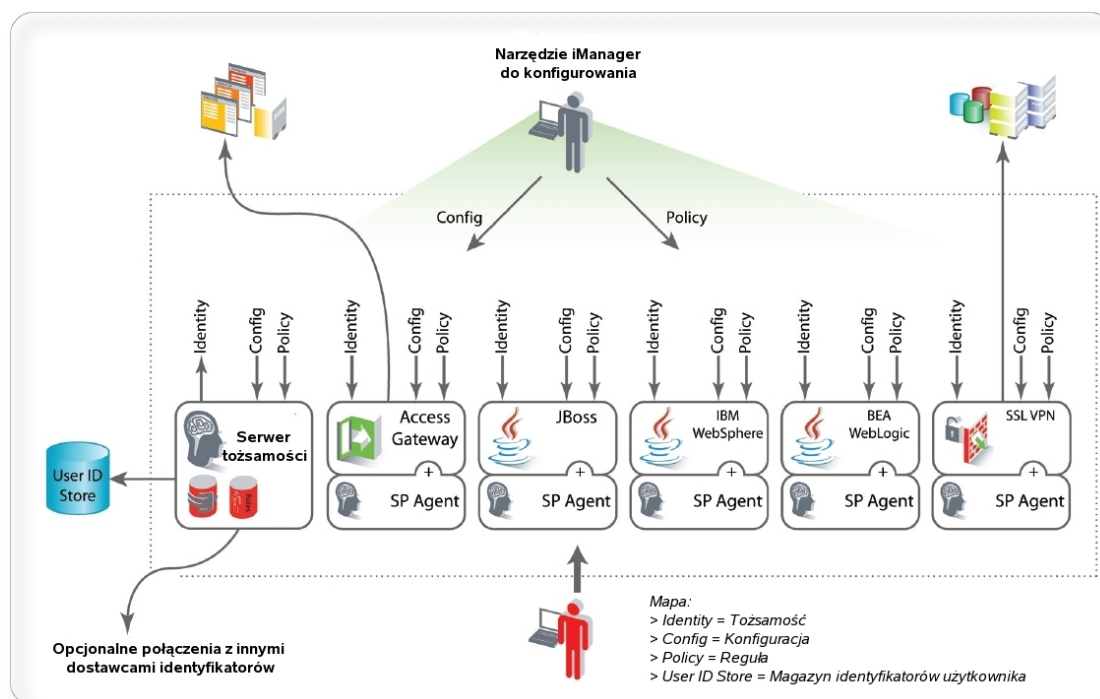
Novell Access Manager pozwala:

- 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.

Novell Access Manager jest idealnym rozwiązaniem dla firm wymagających autoryzacji dostępu do usług udostępnianych przez HTTP lub innymi drogami. Podstawowym zastosowaniem oprogramowania Access Manager w tym zakresie jest zarządzanie dostępem (uwierzytelnianie i autoryzowanie użytkowników) oraz federowanie tożsamości.

Komponenty produktu Novell Access Manager

Pełna integracja komponentów oprogramowania Novell Access Manager zapewnia kontrolę dostępu na wszystkich poziomach, co jest przedstawione na poniższym rysunku.



Rysunek 1. Komponenty oprogramowania Novell Access Manager

Komponenty produktu Novell Access Manager są pokazane 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 oprogramowaniu Novell Access Manager

Podstawowe możliwości oprogramowania Novell Access Management 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. Stosowanie reguł można uprościć poprzez wykorzystanie ról, a procesy zewnętrzne można włączyć za pośrednictwem interfejsu programowania reguł (*Policy API*).

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 SAML (wersja 1.1 i 2.0), WS-Federation, Liberty Alliance i Information Cards. Podobnie jak w przypadku pozostałych 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 oraz do uproszczenia zarządzania regułami.

Przedsiębiorstwa mogą używać udostępnianych przez serwer tożsamości profili (pracownika lub 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 scentralizowanych funkcji zarządzania tożsamością i regułami oprogramowania Novell Access Manager, udostępniający usługi uwierzytelniania, autoryzacji, jednokrotnego logowania WWW oraz personalizacji w dowolnym standardowym serwerze WWW.

Brama dostępu umożliwia przedsiębiorstwu 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 żadnych modyfikacji, do obsługi nowych standardów tożsamości.

Przykładem jest oferowana przez bramę funkcja „wstawiania tożsamości” (*Identity Injection*), która może wykorzystać platformę usług internetowych Liberty Alliance Web Services Framework do wydobywania informacji o tożsamości oraz wstawiania ich do nagłówków WWW lub ciągów znaków zawierających zapytania.

Agenty serwera aplikacji Javy

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

Service Provider Agent (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 również dostawcy tożsamości połączenie łańcuchowe z innymi dostawcami tożsamości. Proces ten, określany jako *IDP proxying*, ułatwia przedsiębiorstwom tworzenie grup powiązanych ze sobą dostawców tożsamości.

Secure Sockets Layer Virtual Private Network (SSL VPN)

SSL VPN zapewnia bezpieczny dostęp do aplikacji nieodparty na HTTP. 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 i wyboru klientów na podstawie ról. Automatyczne czyszczenie pulpitu i bezpieczny folder gwarantują bezpieczeństwo informacji, do których użytkownicy uzyskują dostęp spoza zapory sieciowej.

Mechanizm reguł

Mechanizm reguł (*Policy Engine*) to komponent oprogramowania Novell Access Manager, który zapewnia rozstrzyganie 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.



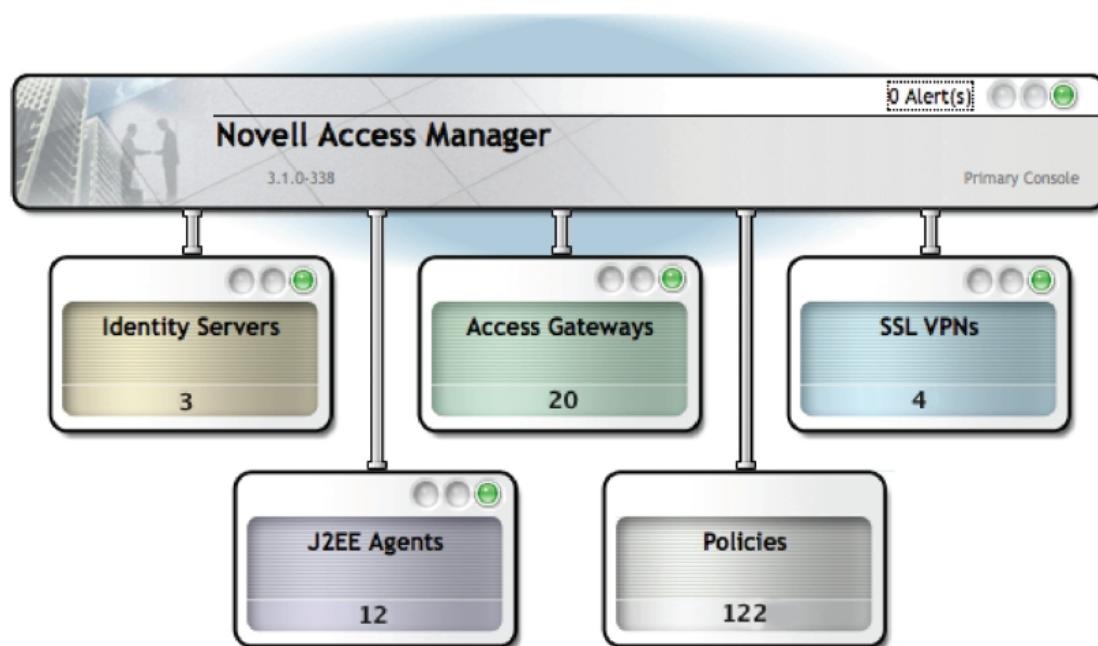
Rysunek 2. Konsola zarządzania oprogramowania Novell Access Manager

Scenariusze wdrożenia i wykorzystania

W tym rozdziale opisane są różne scenariusze wdrożenia i użycia produktu 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*).



Rysunek 3. Deska rozdzielcza rozwiązania Novell Access Manager (Primary Console: Konsola główna, Identity Servers: Serwery tożsamości, Access Gateways: Bramy dostępu, Policies: Reguły).

Ilustracja 3 przedstawia widok najwyższego poziomu udostępniany przez interfejs administracyjny oprogramowania Novell Access Manager. Na poziomie tym wszyscy administratorzy mogą widzieć status wszystkich urządzeń i reguł, a także wszystkie ewentualne ostrzeżenia lub alarmy.

W każdym polu widoczna jest łączna liczba urządzeń oraz zagregowany status alarmu w danej kategorii. Pole serwerów tożsamości informuje na przykład, że w systemie znajdują się trzy takie serwery, wszystkie w pełni funkcjonalne. Status ten jest reprezentowany przez zielone kółko na trzeciej pozycji od lewej.

Pole kontrole reguł (*Policies*) różni się od pozostałych, ponieważ nie ma w nim wskaźników statusu alarmu. Umożliwia ono autoryzowanemu administratorowi (tj. kontrolującemu dostęp do sekcji interfejsu administracyjnego dotyczącej zarządzania regułami) tworzenie i edytowanie reguł przypisanych do określonych komponentów oraz zarządzanie nimi. Sekcja zarządzania regułami (*Policy Administration*) stwarza dodatkową warstwę kontroli dostępu przez administratora. Reguły można podzielić na jedną lub wiele grup, które zostaną przypisane administratorom reguł (*Policy Administrators*). Ułatwia to podział obowiązków pomiędzy tych administratorów oraz rozwiązywanie wiele problemów dotyczących zgodności z przepisami.

Administrowanie regułami w oprogramowaniu Novell Access Manager

Dostępność funkcji administrowania regułami w skali całego systemu jest ogromną zaletą rozwiązania Novell Access Manager, dla której zdecydowanie warto go wdrożyć.

Reguły są oparte na punktach egzekwowania reguł (PEP – *Policy Enforcement Points*). Dla każdego komponentu oprogramowania Novell Access Manager jest zdefiniowanych kilka takich punktów. W celu utworzenia reguły administrator deklaruje najpierw, który punkt PEP będzie kontrolowany przy jej użyciu. Taka wstępna deklaracja ma 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 to samo, dzięki czemu utrzymanie mechanizmu reguł wymaga kontroli tylko jednego elementu.*
- *Administrowanie regułami umożliwia także przydzielanie reguł do różnych komponentów produktu Access Manager. Taki przydział obowiązuje tak długo, dopóki dany komponent obsługuje punkt PEP, na którym może działać dana reguła. Administrator ma do dyspozycji narzędzia pozwalające na sprawdzenie, które reguły są używane przez poszczególne urządzenia.*
- *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 konfigurowanie rozdzielnie obowiązków pomiędzy pracowników odpowiedzialnych za utrzymywanie reguł. 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 reguł dla serwera tożsamości.*
- *Novell Access Manager rejestruje wszystkie czynności związane z regułami i generuje raporty dotyczące zgodności z przepisami. Dotyczy to takich czynności, jak tworzenie, modyfikowanie, wyłączanie i ostateczne usuwanie reguł. Informacje z dziennika można wyszukiwać za pomocą zapytań, co pozwala na przykład na określenie, jaka reguła rządziła dostępem w dowolnym momencie.*

Konfigurowanie federacyjne w oprogramowaniu Novell Access Manager

Niektóre tradycyjne systemy wymagają, aby przedsiębiorstwo przechowywało wszystkie informacje dotyczące tożsamości w określonym katalogu i formacie. Wszyscy użytkownicy takiego systemu muszą mieć konto w takim katalogu zanim zaczną korzystać z dostępnych usług. Novell Access Manager umożliwia automatyczne konfigurowanie tego rodzaju kont bez konieczności samodzielnego, ręcznego rejestrowania się przez użytkowników w katalogu tradycyjnego systemu.

W rozwiązaniu Novell Access Manager konfigurowanie federacyjne jest realizowane poprzez serwer tożsamości, który pełni funkcję dostawcy usług (*Service Provider*). Jeśli zostanie on przygotowany do automatycznego konfigurowania kont użytkowników, weryfikuje najpierw każde żądanie uwierzytelnienia w celu ustalenia, czy katalog tradycyjnego systemu zawiera konto użytkownika. Jeżeli tak, to operacja uwierzytelniania przebiega normalnie. W przeciwnym wypadku 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 nagłówków niezbędne do zapewnienia użytkownikom bezproblemowego dostępu do tradycyjnych systemów internetowych.

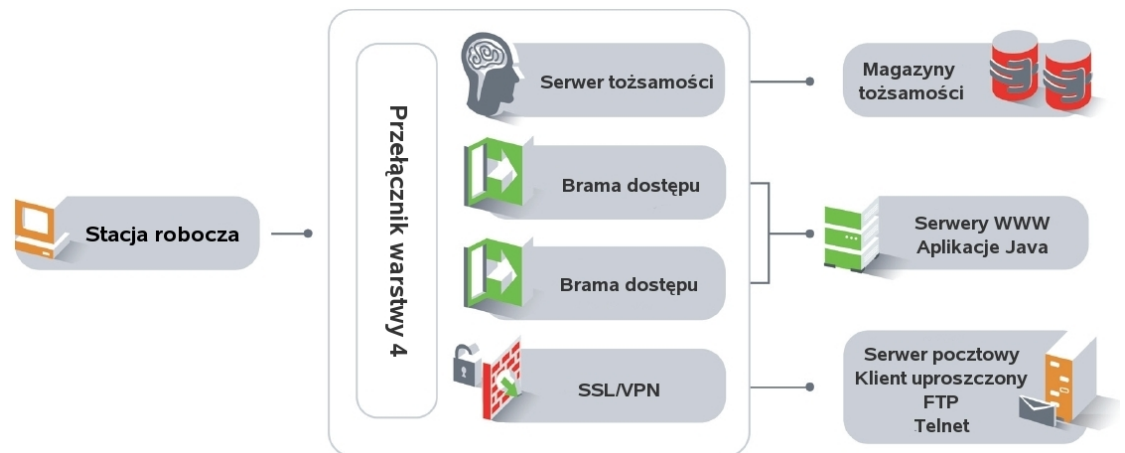
W niektórych przypadkach przedsiębiorstwa wymagają, aby tradycyjne usługi internetowe używały aliasu identyfikatora użytkownika i hasła. Novell Access Manager umożliwia stosowanie dowolnej kombinacji atrybutów z jednego lub więcej magazynów tożsamości w charakterze identyfikatora użytkownika i hasła.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

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:

- *Serwer tożsamości zapewnia zarządzanie tożsamością w oparciu o reguły, w tym zarządzanie tożsamościami i/lub rolami sfederowanymi.*
- *Bramy dostępu zapewniają kontrolę dostępu do zasobów i aplikacji opartych na Internecie, przy użyciu tożsamości zarządzanych przez serwer tożsamości. Pomaga w tym m.in. komponent Novell Access Manager Policy, który umożliwia definiowanie praw dostępu do zasobów lokalnych na podstawie reguł i ról.*
- *SSL VPN zapewnia bezpieczny, oparty na tożsamości i rolach dostęp do pozostałych zasobów i aplikacji poza zaporą sieciową.*



Rysunek 4. Novell Access Manager — schemat ogólny

Zarządzanie dostępem a federacja oparta na standardach

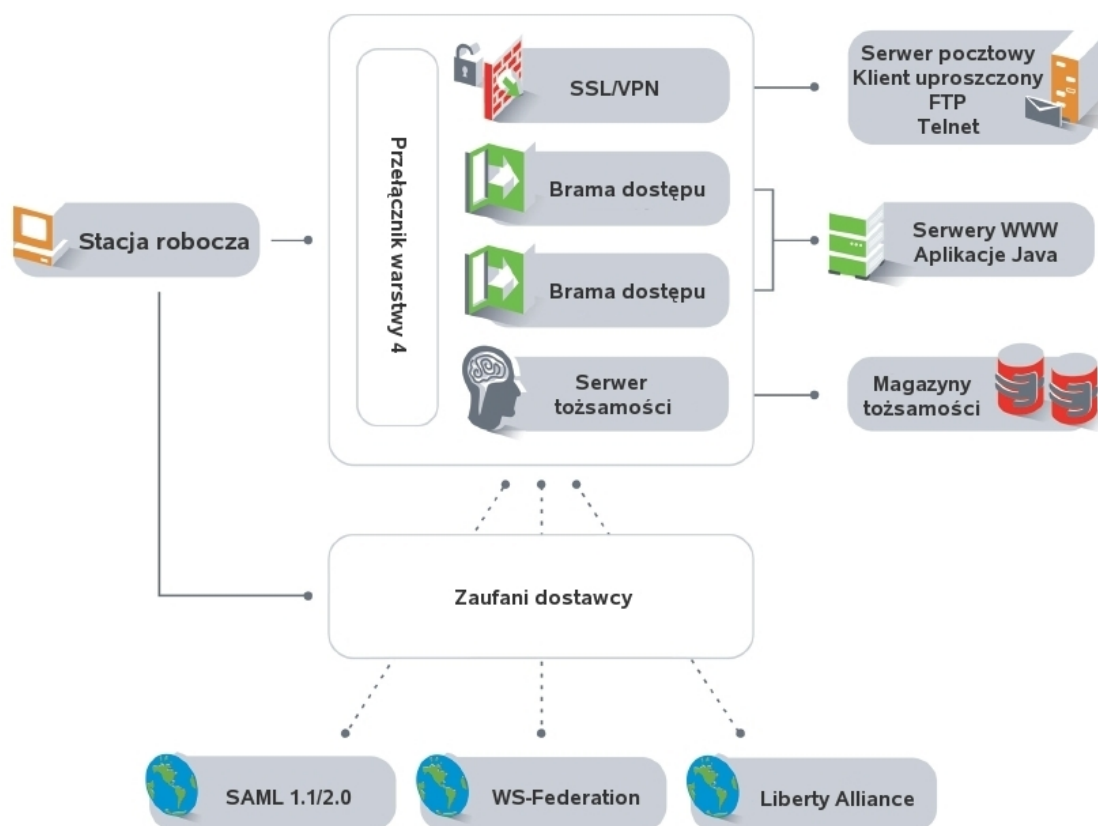
Każde wdrożenie produktu Novell Access Manager obejmuje jeden lub więcej serwerów tożsamości, które koordynują tożsamości użytkowników we wszystkich fazach ich cyklu życia, w tym federację z innymi dostawcami tożsamości. Oznacza to, że pomyślne uwierzytelnienie u jednego zaufanego partnera zapewnia uwierzytelnienie również u innych zaufanych, sfederowanych partnerów. Na przykład pomyślne uwierzytelnienie w serwerze tożsamości systemu Novell Access Manager może być

honorowane przez inny system, który nie ma nic wspólnego z systemem Novell Access Management. Może to zapewnić użytkownikowi dostęp do zasobów takiego oddzielnego systemu bez konieczności uwierzytelniania się w nim.

Serwer tożsamości rozwiązania Novell Access Manager jest w pełni zgodny ze specyfikacją standardu Liberty Alliance i WS-Federation, przy czym 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 za pośrednictwem serwera tożsamości. Każda taka sfederowana tożsamość jest przekazywana do obszaru zaufanego (*trust perimeter*) menedżera dostępu zgodnie z regułami lokalnymi.

Gdy zostanie skonfigurowana umowa federacji z systemami zewnętrznymi, pozostaje ona w mocy zgodnie z regułami wygasania, które są monitorowane i egzekwowane przez rozwiązanie 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 za pośrednictwem WWW, wypełnionych formularzy, nagłówków HTTP bądź innymi metodami. Dzięki temu system zarządzania tożsamością udostępnia bogate możliwości funkcjonalne oraz może być w pełni zarządzany zarówno przez przedsiębiorstwo, jak też indywidualnych użytkowników.



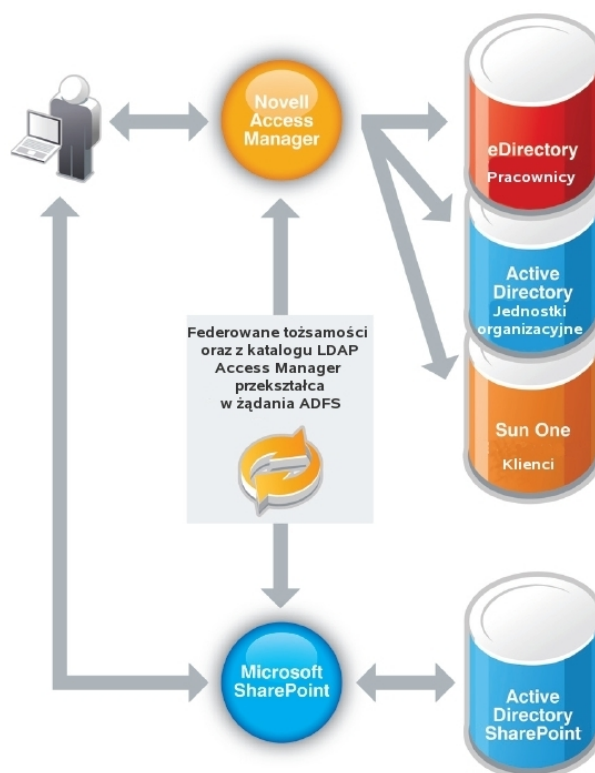
Rysunek 5. Jednokrotne zalogowanie obejmujące systemy wewnętrzne oraz różne systemy sfederowane lub zaufane

Zarządzanie dostępem a federacja korporacyjna — uproszczony dostęp do systemu Microsoft SharePoint

Funkcje federacyjne dostępne w rozwiązaniu Novell Access Manager można również wykorzystać, aby uprościć dostęp do zasobów przedsiębiorstwa, takich jak Microsoft SharePoint, zwłaszcza gdy tożsamości użytkowników są umieszczone w wielu magazynach LDAP, a zaufani partnerzy potrzebują dostępu poprzez komponent Identity Federation.

Dzięki wbudowanej obsłudze standardu WS-Federation, rozwiązanie Novell Access Manager można zintegrować z usługami federacji aktywnych katalogów (*Active Directory Federation Services*), aby umożliwić uwierzytelnianie oparte na żądaniach dostępu do systemu Microsoft SharePoint.

W rezultacie administratorzy systemu SharePoint mogą odwzorowywać otrzymane żądania na grupy SharePoint, co w dużej mierze eliminuje potrzebę tworzenia indywidualnych tożsamości w magazynie tożsamości SharePoint.



Rysunek 6. Uwierzytelnianie w MS SharePoint oparte na żądaniach

Rejestrowanie danych dla celów zgodności z przepisami

Novell Access Manager udostępnia ważne funkcje rejestrowania danych w celu zapewnienia zgodności z przepisami. Każdy komponent tworzy zapisy w dzienniku (logu), które mogą być przechowywane lokalnie lub odbierane przez narzędzie Novell Sentinel.

Wieloczynnikowa ochrona zasobów

Specyfikacja reguły kontroluje dostęp do wszystkich zasobów chronionych przez program Novell Access Manager. Oznacza to, że uzyskanie dostępu do konkretnego zasobu może wymagać spełnienia więcej niż jednej reguły. Każda reguła może wygenerować inny czynnik kontroli tożsamości niezależnie od specyfikacji pozostałych reguł. Pozwala to na uzyskanie wieloczynnikowej ochrony zasobów z bardzo szczegółowym rozróżnianiem na poziomie specyfikacji reguły.

Najczęściej zadawane pytania (FAQ)

Czy używane przeze mnie oprogramowanie Novell iChain będzie współpracować z nową bramą dostępu?

Starsze wdrożenia oprogramowania Novell iChain będą funkcjonować jak dotychczas, ale nie stanowią one części nowej konsoli administracyjnej systemu Novell Access Manager. W przypadku przełączenia awaryjnego za pośrednictwem przełącznika warstwy 4 między oprogramowaniem iChain a bramą dostępu użytkownik będzie musiał ponownie się uwierzytelnić, aby można było wywołać właściwe specyfikacje reguł. Dokumentacja produktu Novell Access Manager zawiera strategię współistnienia oprogramowania iChain, która przewiduje jednokrotne logowanie do systemów iChain i Novell Access Manager. Usługi będą stopniowo przenoszone z systemu iChain do Novell Access Manager.

Czy mogę zarządzać wieloma bramami dostępu jako grupą, nawet jeśli każda z nich ma inny adres IP?

Tak. Adresy IP są obsługiwane w taki sposób, że można bez problemu zarządzać grupami bram dostępu. Administratorzy definiują klastry bram dostępu, co pozwala na zarządzanie wieloma urządzeniami z jednego punktu.

Czy Novell Access Manager pomoże mi w zarządzaniu dostępem do systemu SharePoint dla różnych społeczności użytkowników?

Tak. Dzięki wbudowanej obsłudze standardu WS-Federation, rozwiązanie Novell Access Manager można zintegrować z usługami federacji aktywnych katalogów (Active Directory Federation Services), aby umożliwić uwierzytelnianie oparte na żądaniach dostępu do systemu SharePoint. Eliminuje to konieczność zarządzania indywidualnymi tożsamościami w magazynie tożsamości SharePoint.

Czy moi użytkownicy muszą uwierzytelniać się na serwerze SSL VPN po uwierzytelnieniu w aplikacjach internetowych chronionych przez oprogramowanie Novell Access Manager?

Nie, użytkownik nie musi się uwierzytelniać na serwerze SSL VPN, jeżeli uwierzytelnił się w systemie Novell Access Manager. Będzie jednak musiał uwierzytelnić się w każdej aplikacji, chyba że został wdrożony system jednokrotnego logowania obejmujący całe przedsiębiorstwo, taki jak Novell SecureLogin.

Czy mogę zintegrować rozwiązanie Novell Access Manager z innymi usługami federacyjnymi w moim przedsiębiorstwie?

Tak. Rozwiązanie Novell Access Manager (zarówno jako dostawca, jak i klient) może zostać zintegrowane z każdą usługą zgodną ze standardami SAML, WS-Federation lub Liberty Alliance.

Czy mogę skonfigurować serwer tożsamości tak, by akceptował uwierzytelnianie przez proxy?

Tak, serwer tożsamości obsługuje uwierzytelnianie przez proxy.

Więcej informacji

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

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-PL2033-003 | 06/10 | © 2010 Novell Inc. Wszelkie prawa zastrzeżone. Novell, logo Novell, logo N i iChain są zastrzeżonymi znakami towarowymi, a Access Manager, eDirectory i Sentinel są znakami towarowym firmy Novell Inc. w Stanach Zjednoczonych i innych krajach.

* Pozostałe znaki towarowe są własnością odpowiednich podmiotów.