









Zarządzanie tożsamością i bezpieczeństwem

Przegląd rozwiązań firmy Novell do integracji systemów,
automatyzacji procesów i bezpiecznego dostępu

Novell.

Spis treści:

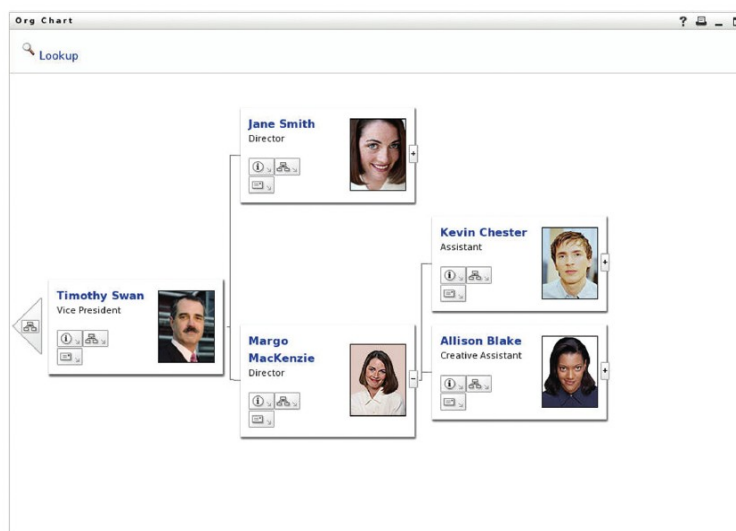
3		Novell Identity Manager
6		Novell Access Manager
8		Sentinel firmy Novell
10		Novell Identity Assurance Solution
12		Novell SecureLogin
14		Novell Storage Manager
16		Novell eDirectory
18		Projekt Bandit



Novell Identity Manager

Uproszczenie wyposażania użytkowników w dostęp do informacji i zasobów oraz zarządzania hasłami

Każde przedsiębiorstwo gromadzi szczegółowe dane o pracownikach, klientach, partnerach, projektach itp. Dane te często znajdują się w różnych systemach i wymagają częstej aktualizacji. Gdyby te zmiany miały być wykonywane ręcznie przez pracowników działu informatycznego, zapewnienie aktualności informacji we wszystkich systemach byłoby bardzo kosztowne, a prawdopodobieństwo błędów przy wprowadzaniu danych byłoby ogromne. Novell Identity Manager rozwiązuje ten problem, gdyż automatyzuje procesy zarządzania tożsamością. Modyfikacje danych w systemie głównym są niemal natychmiast odzwierciedlane we wszystkich pozostałych systemach bez konieczności ręcznej interwencji pracowników. Użytkownicy mogą korzystać z danych (do których są upoważnieni) szybko i bezpiecznie, a nawet samodzielnie zmieniać własne hasła bez obciążania tym pracowników działu informatycznego. Novell Identity Manager to bardzo wydajne rozwiązanie, które zapewnia przedsiębiorstwu oszczędności finansowe, zmniejsza złożoność systemów oraz ogranicza ryzyko związane z ręcznymi procesami aktualizacji danych.



Rys. 1. Łatwy w użyciu spis pracowników ułatwia zorientowanie się w organizacji przedsiębiorstwa

Cechy i funkcje

- Automatyizacja konfigurowania kont i uprawnień użytkowników oraz zarządzania hasłami
- Szerokie możliwości korzystania z oprogramowania w trybie samoobsługi
- Możliwość rejestracji użytkowników w trybie samoobsługi
- Automatyizacja procedur (*workflow*) związanych z zatwierdzaniem przyznawania uprawnień
- Rygorystyczne egzekwowanie reguł dotyczących haseł
- Dwukierunkowa synchronizacja haseł
- Administrowanie tożsamością w oparciu o role i stanowisko pełnione przez osobę w organizacji
- Projektowanie i współużytkowanie nowych procedur (*workflow*) bez ręcznego kodowania
- Tworzenie i testowanie reguł „na żywo”, bez ryzyka dla działających systemów
- Automatyczne generowanie dokumentacji ułatwiającej zapewnienie zgodności z regulacjami i przepisami
- Skrócenie czasu potrzebnego do wdrożenia rozwiązania dzięki automatycznemu czyszczeniu danych (*data scrubbing*)
- Dostępność narzędzi do sprawdzania poprawności reguł synchronizacji danych o tożsamości

- Automatyczne przydzielanie uprawnień na podstawie ról pełnionych przez osobę w organizacji
- Monitorowanie ról dla potrzeb raportowania zgodności z regulacjami i przepisami
- Tworzenie raportów na temat uprawnień dostępu wszystkich użytkowników w formie przygotowanej do audytu
- Możliwość wykorzystania własnych spisów pracowników i schematów organizacyjnych przedsiębiorstwa

Obsługiwane systemy i aplikacje

Bazy danych	SAP HR	Inne systemy i standardy
IBM DB2	SAP R/3 4.6 i SAP Enterprise Systems (BASIS)	Pliki tekstowe z separatorami
IBM Informix	SAP Web Application Server (Web AS) 6.20	DSML
JDBC	Siebel	Remedy (helpdesk)
Microsoft SQL Server		Schools Interoperability Framework (SIF)
MySQL		SOAP
Oracle	Magistrala usług przedsiębiorstwa	SPML
Sybase	BEA	
	IBM WebSphere MQ	Centrale abonenckie (PBX)
Katalogi	JBoss	Avaya PBX
Critical Path InJoin Directory	OpenJMS	
IBM Tivoli Directory Server (wcześniej IBM SecureWay Directory Server)	Oracle	
iPlanet Directory Server	Sun	
LDAP	TIBCO	
Microsoft Active Directory	Systemy mainframe	
Microsoft Windows NT Domains	CA-ACF2	
Netscape Directory Server	CA-Top Secret	
NIS	RACF	
NIS+		
Novell eDirectory	Systemy klasy średniej	
Novell NDS	OS/400 (AS/400)	
Oracle Internet Directory		
Sun ONE Directory Server	Systemy operacyjne	
	Debian Linux	
Systemy poczty elektronicznej	FreeBSD	
Lotus Notes	HP-UX	
Microsoft Exchange 2000, 2003, 2007	IBM AIX	
Microsoft Exchange 5.5	Microsoft Windows 2000, 2003	
Novell GroupWise	Microsoft Windows NT 4.0	
	Red Hat Linux	
	Red Hat Linux Advanced Server i Red Hat Enterprise Linux	
Aplikacje korporacyjne	Solaris	
Baan	Novell SUSE Linux Enterprise Server	
J.D. Edwards	Pliki systemu UNIX — /etc/passwd	
Lawson		
Oracle		
PeopleSoft		

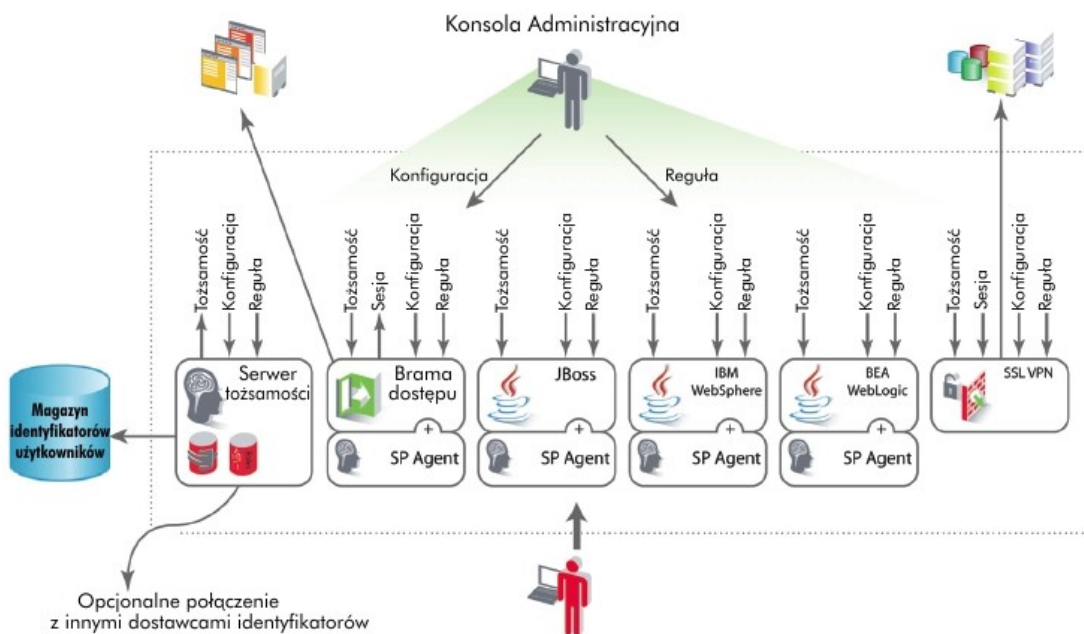
Novell Access Manager

Zapewnienie nieskomplikowanego i bezpiecznego dostępu do webowych i firmowych zasobów przedsiębiorstwa, a równocześnie ochrona organizacji przed atakami

Pracownicy, partnerzy i klienci przedsiębiorstwa bądź instytucji potrzebują często dostępu do sieci przedsiębiorstwa z dowolnego miejsca oraz w dowolnym czasie. Jednak jednocześnie konieczna jest ochrona sieci przed dostępem konkurencji i przestępców. Przedsiębiorstwa muszą zorganizować więc bezpieczny, a przy tym niekłopotliwy dostęp do zasobów sieci, dla którego nie będą przeszkodą bariery techniczne i organizacyjne. Novell Access Manager pozwala sprostać temu wyzwaniu. Zapewnia on użytkownikom dostęp do zasobów bez zbędnego ograniczania bezpieczeństwa i kontroli. W celu ochrony systemów przedsiębiorstwa, Access Manager stosuje zaawansowane narzędzia i technologie, w tym różne metody uwierzytelniania, szyfrowanie danych, mechanizm jednokrotnego logowania do sieci przez WWW oraz bezklientową wirtualną sieć prywatną (VPN) opartą na protokole SSL. Access Manager stanowi ściśle zintegrowane rozwiązanie bezpieczeństwa, pozwalające przedsiębiorstwu zminimalizować ryzyko, a równocześnie wzmocnić relacje z klientami i partnerami.

Cechy i funkcje

- Zmniejszenie złożoności oraz obniżenie kosztów zarządzania dostępem
- Zabezpieczony dostęp do sieci WWW i aplikacji korporacyjnych
- Autoryzacja dostępu w oparciu o role użytkowników
- Jednokrotne logowanie do aplikacji internetowych
- Wielopoziomowe uprawnienia dostępu do wspieranych serwerów J2EE
- Obsługa zaawansowanych metod uwierzytelniania
- Obsługa federacji tożsamości (wsparcie dla SAML 1.1 / 2.0 oraz Liberty Alliance)
- Obsługa aprowizacji dla tożsamości sfederowanych, co umożliwia automatyczne generowanie kont użytkowników na żądanie z federacji
- Obsługa magazynów tożsamości Novell eDirectory, Microsoft Active Directory i Sun ONE.



Rys. 1. Ogólny widok komponentów oprogramowania Novell Access Manager

Access restricted

You are attempting to access a site to which you have not been granted access. To request access, enter the justification for your request and click the 'request access' button below. An access request workflow will be sent to your manager and/or the resource owner to approve or deny your request.

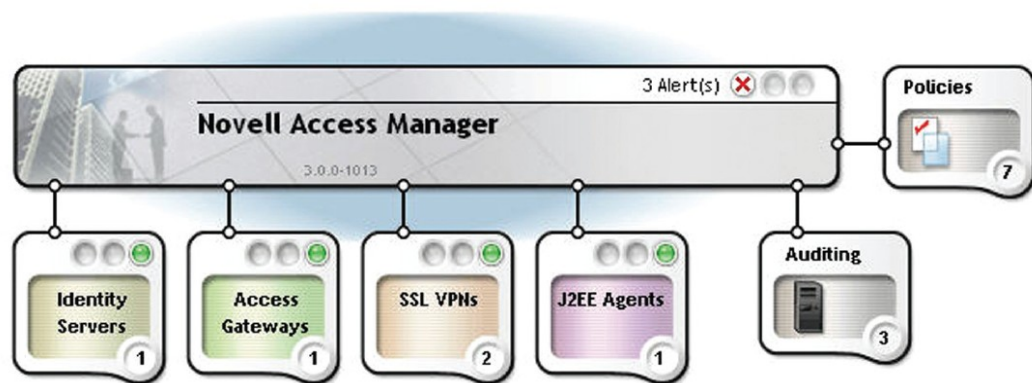
Entitlement Name: Training Online & Books (*self approve)
Entitlement Description:

Access to the SkillPort site for access to online books and training resources.

Access Policy: - Default for regular employees, interns, and Novell temp employees - Manager approval for all other worker types

Justification:

Rys. 2. Obsługa procedur (workflow) w oparciu o produkty Novell Access Manager i Novell Identity Manager



Rys. 3. Graficzny interfejs administratora udostępnia wgląd w status poszczególnych komponentów za pomocą specjalnej tablicy rozdzielczej (dashboard)

DX MEDICAL
Benefits Portal

Username:

Password:

Federated Logins:

Rys. 4. Łatwy dostęp do sfederowanych serwisów internetowych partnerów



Sentinel firmy Novell

Automatyczne i nieustanne monitorowanie zdarzeń związanych z bezpieczeństwem oraz zgodnością z regulacjami i przepisami

Każde przedsiębiorstwo codziennie zbiera informacje o zdarzeniach zachodzących w wykorzystywanych urządzeniach sieciowych, systemach i aplikacjach. Ale czy dział IT ma dość czasu i ludzkich zasobów, aby ręcznie przeglądać, kojarzyć i oceniać wszystkie takie informacje? A co z potencjalnymi zagrożeniami dla bezpieczeństwa? Przedsiębiorstwo nie musi się kłopotać takimi problemami, jeśli używa oprogramowania Sentinel firmy Novell. Zapewnia ono pełny wgląd w informację o stanie bezpieczeństwa sieci przedsiębiorstwa, a także automatyzuje monitorowanie zasobów informatycznych pod kątem efektywności oraz analizuje korelacje w napływających danych, dzięki czemu umożliwia wykrywanie i eliminowanie zagrożeń w czasie rzeczywistym, zanim wpłyną one negatywnie na działalność przedsiębiorstwa. Ponadto Sentinel zapewnia możliwość tworzenia dokumentacji wymaganej przez restrykcyjne prawo, regulacje i przepisy branżowe.

Cechy i funkcje

- Widok danych o zdarzeniach prezentowany w czasie rzeczywistym dzięki konfigurowanym tablicom rozdzielczym
- Obniżenie kosztów zapewnienia bezpieczeństwa i zgodności z regulacjami i przepisami
- Sprawnie i skuteczne zarządzanie ryzykiem związanym z bezpieczeństwem systemów IT
- Szybkie wykrywanie i rozwiązywanie incydentów
- Raportowanie zarówno dla potrzeb bezpieczeństwa jak i dla potrzeb zapewnienia zgodności z przepisami
- Monitorowanie zgodności z wewnętrznymi regułami oraz dokumentowanie zgodności dla zewnętrznych podmiotów, takich jak organy kontrolne, partnerzy i klienci
- Umożliwienie skoncentrowania zasobów IT na innych krytycznych przedsięwzięciach informatycznych i biznesowych
- Szybkie wykrywanie ataków lub naruszeń zgodności z regulacjami i przepisami dzięki elastycznym mechanizmom kojarzenia informacji w pamięci operacyjnej
- Korelowanie przy użyciu dynamicznych list, co umożliwia doskonalsze zestawianie z wyselekcjonowanymi danymi historycznymi dla potrzeb analizy danych przyszłych
- System inteligentnego gromadzenia danych o zdarzeniach, zapewniający ich zbieranie, analizę składniową, normalizację oraz wzbogacanie
- Reagowanie na incydenty związane z bezpieczeństwem i zgodnością z użyciem w pełni dostosowywanego systemu obsługi procedur (*workflow*)
- Tablice rozdzielcze i raporty dla kierownictwa pozwalające na badanie zgodności z regulacjami i przepisami, takimi jak Sarbanes-Oxley, HIPAA, PCI i inne
- Uproszczone wdrażanie i zarządzanie produktami, sprawdzanie kondycji systemu (*health check*) dzięki narzędziom z serii Event Source Management (narzędzia do zarządzania danymi źródłowymi o zdarzeniach).

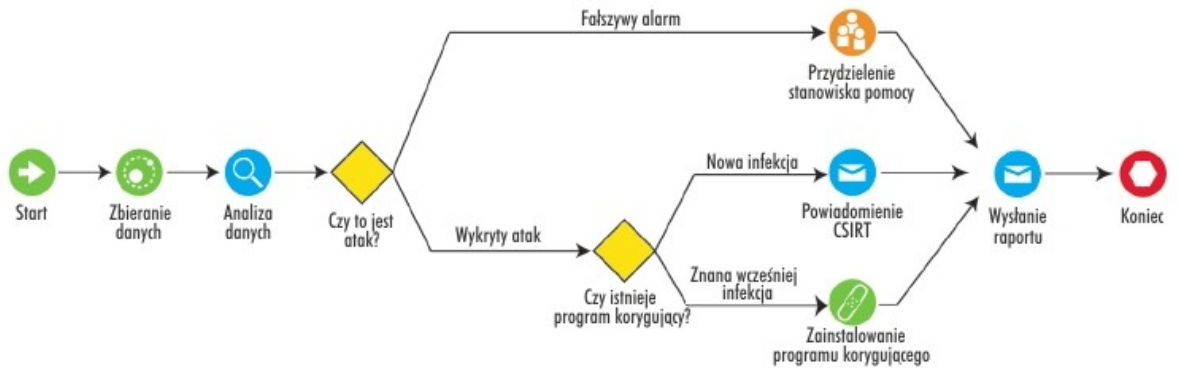
Obsługiwane platformy

Systemy operacyjne

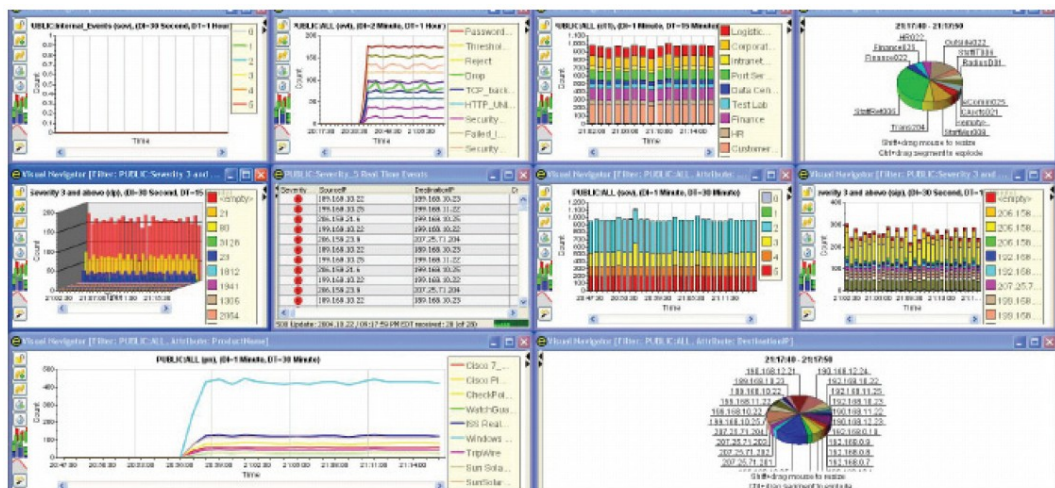
Novell SUSE Linux Enterprise Server 9 (32-bit.)
Novell SUSE Linux Enterprise Server 10 (32- i 64-bit.)
Red Hat Enterprise Linux 3 (32-bit.)
Solaris 9 (32- i 64-bit.)
Solaris 10 (64-bit.)
Windows 2003 (32- i 64-bit.)

Bazy danych

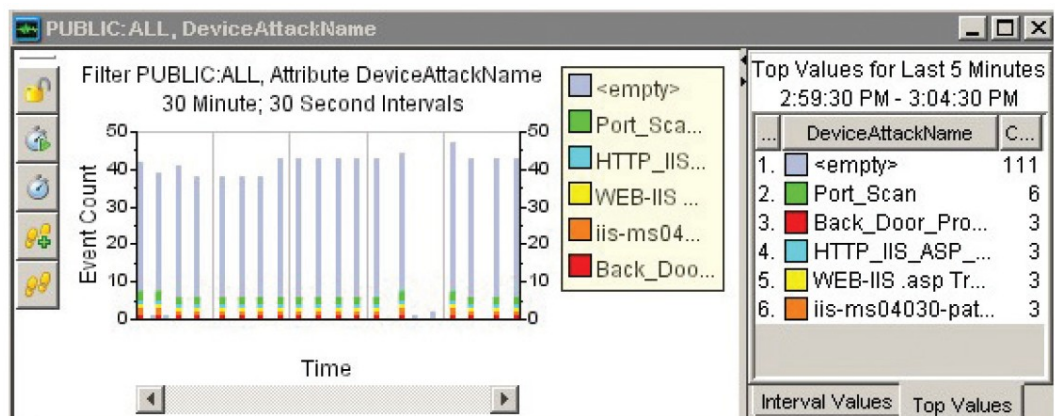
Microsoft SQL Server 2005
Oracle 9i
Oracle 10g wraz z Real Application Clusters (RAC)



Rys. 1. Analiza danych o zdarzeniach umożliwia szybkie reagowanie oraz działanie z wyprzedzeniem (CSIRT = Computer Security Incident Response Team)



Rys. 2. Jeden widok prezentujący cały system



Rys. 3. Filtrowanie widoku zdarzeń



Novell Identity Assurance Solution

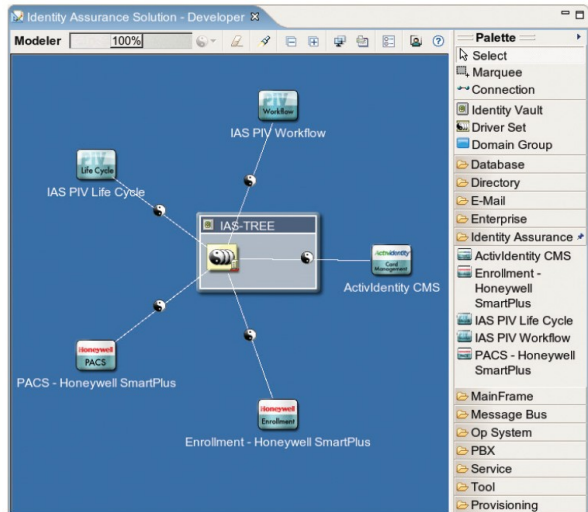
Zabezpieczenie najbardziej poufnych informacji dzięki konwergencji oprogramowania i sprzętu, zapewniającej zintegrowany, kompleksowy system kontroli z wykorzystaniem kart tożsamości

Wiele współczesnych przedsiębiorstw i instytucji posiada poufne, a niekiedy nawet ściśle tajne informacje, a także jest zobowiązanych do zapewnienia zgodności z coraz większą liczbą regulacji i przepisów dotyczących kontroli tożsamości. Na przykład amerykańskie federalne agencje rządowe muszą zapewnić zgodność z surowymi wymaganiami bezpieczeństwa nałożonymi przez Dyrektywę Prezydencką nr 12 ws. bezpieczeństwa wewnętrznego (Homeland Security Presidential Directive 12 — HSPD-12). Novell Identity Assurance Solution ułatwia przedsiębiorstwom i instytucjom zapewnienie bezpieczeństwa informacji oraz zapewnienie zgodności z przepisami. Rozwiązanie to udostępnia najlepsze w swych kategoriach usługi katalogowe, uwierzytelniania, sprawdzania upoważnień, konfigurowania, audytu oraz synchronizacji danych o tożsamości. Identity Assurance Solution spełnia wymagania nakładane przez FIPS 201 (Federal Information Processing Standards — federalne standardy przetwarzania informacji, standard nr 201) w zakresie mechanizmów obsługi procedur (*workflow*), zarządzania tożsamością oraz „cyklu życia” kart kontroli dostępu. Ponadto rozwiązanie umożliwia konwergencję systemów informatycznych i fizycznej kontroli dostępu do pomieszczeń zapewniając zintegrowany, kompleksowy system kontroli oparty na kartach tożsamości.

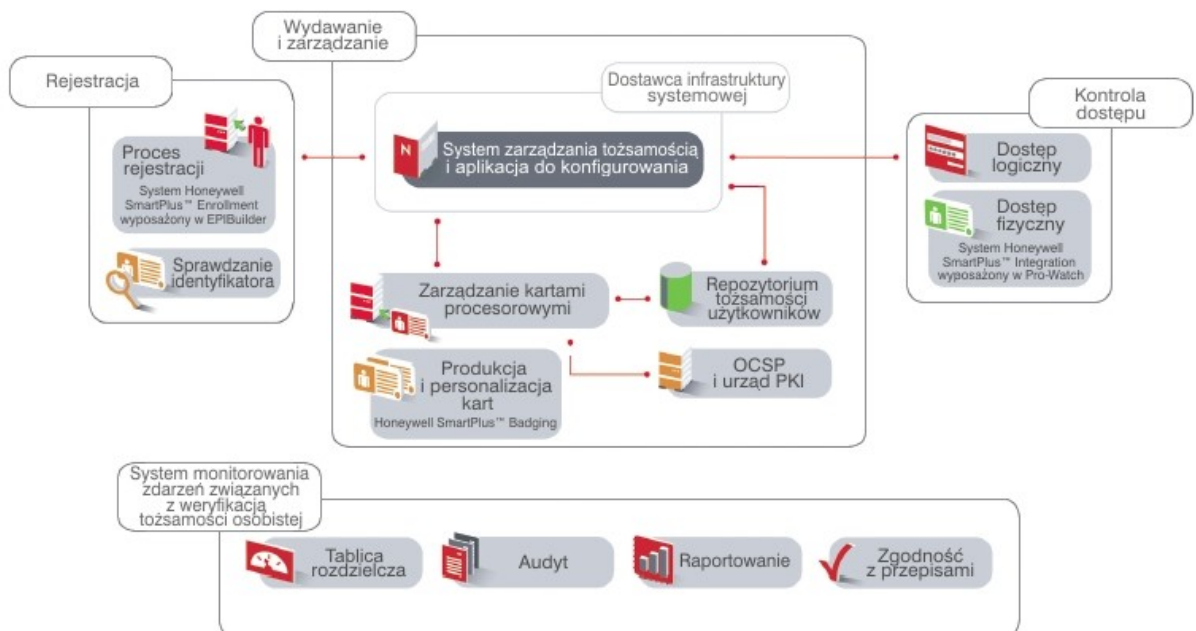
Identity Assurance Solution gromadzi i zarządza ważnymi danymi wymaganymi do obsługi kart tożsamości. W tym celu integruje dane z zewnętrznych systemów uwierzytelniania, systemów zarządzania kartami oraz centrów certyfikacyjnych. Posiada też wbudowany mechanizm (*workflow*) obsługi procedur przyznawania i odbierania uprawnień dostępu. Jest on obsługiwany przez użytkowników (pracownicy działu kadr, przełożeni itd.) i można go łatwo dostosować do potrzeb firmy. Dzięki Identity Assurance Solution użytkownicy posługują się jedną kartą w celu uzyskania dostępu do pomieszczeń oraz różnych aplikacji i systemów.

Cechy i funkcje

- Synchronizacja danych o tożsamości oraz haseł pomiędzy różnymi systemami, zapewniająca użytkownikom uzyskanie jednego zestawu upoważnień dla potrzeb uwierzytelniania do wszystkich potrzebnych aplikacji, baz danych czy zasobów fizycznych (wejście do budynku i wybranych pomieszczeń)
- Obsługa różnych zaawansowanych metod uwierzytelniania, zapewniająca wygodę oraz maksymalne uproszczenie czynności administracyjnych związanych z obsługą haseł
- Obsługa zróżnicowanych poziomów kryteriów dostępu, zapewniająca elastyczne wybieranie odpowiedniego poziomu bezpieczeństwa dla każdego chronionego zasobu
- Zarządzanie kartami tożsamości użytkowników, zapewniające automatyczne (oparte na mechanizmie *workflow*) i wykonywane w czasie rzeczywistym nadawanie, konfigurowanie lub cofanie uprawnień dostępu do wszystkich zasobów przeznaczonych dla poszczególnych osób
- Zarządzanie certyfikatami – obsługa tworzenia, importowania, przechowywania, sprawdzania oraz odwoływania certyfikatów elektronicznych
- Usługi audytu zapewniające śledzenie i monitorowanie dostępu użytkowników, a także skanowanie środowiska sieciowego pod kątem ataków i niewłaściwego użycia zasobów
- Obsługa mobilnych użytkowników, często odłączonych od firmowej sieci, zapewniająca uwierzytelnianie do stacji roboczej przy użyciu karty, nawet jeśli komputer jest odłączony od sieci
- Obsługa wydawania tymczasowych kart procesorowych użytkownikom, którzy zgubili swoją kartę lub jej zapomnieli
- Obsługa automatycznego odnawiania haseł w regularnych odstępach czasu
- Blokowanie komputera w celu uniemożliwienia nieupoważnionego dostępu do niego po wyjęciu karty procesorowej przez użytkownika.



Rys. 1. Funkcja Designer upraszcza konfigurowanie i wdrażanie



Rys. 2. Schemat ogólny rozwiązania Identity Assurance Solution



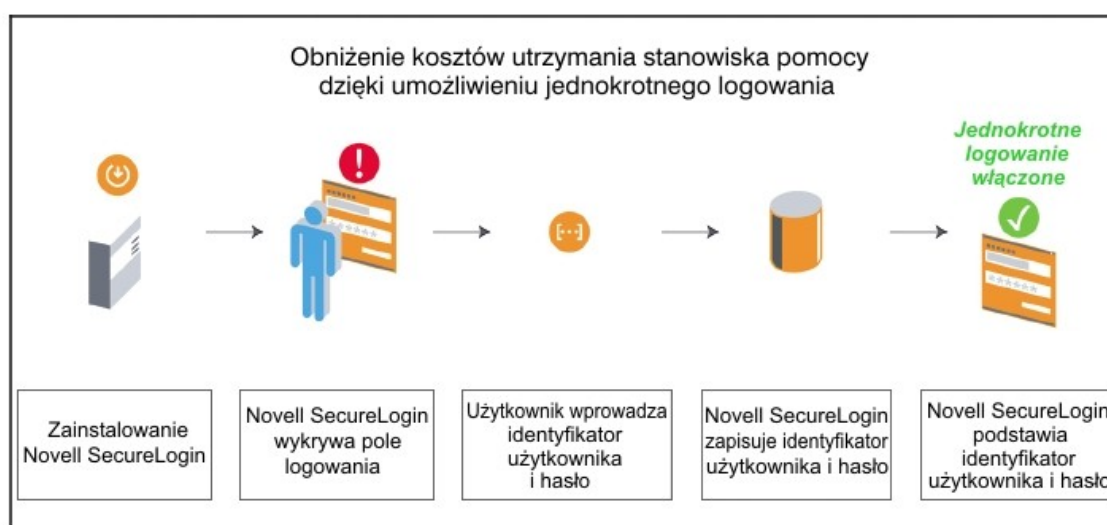
Rys. 3. Czytnik kart procesorowych

Egzekwowanie silnych reguł bezpieczeństwa dotyczących korzystania z haseł bez nakładania na użytkowników wymogu pamiętania wielu identyfikatorów oraz haseł

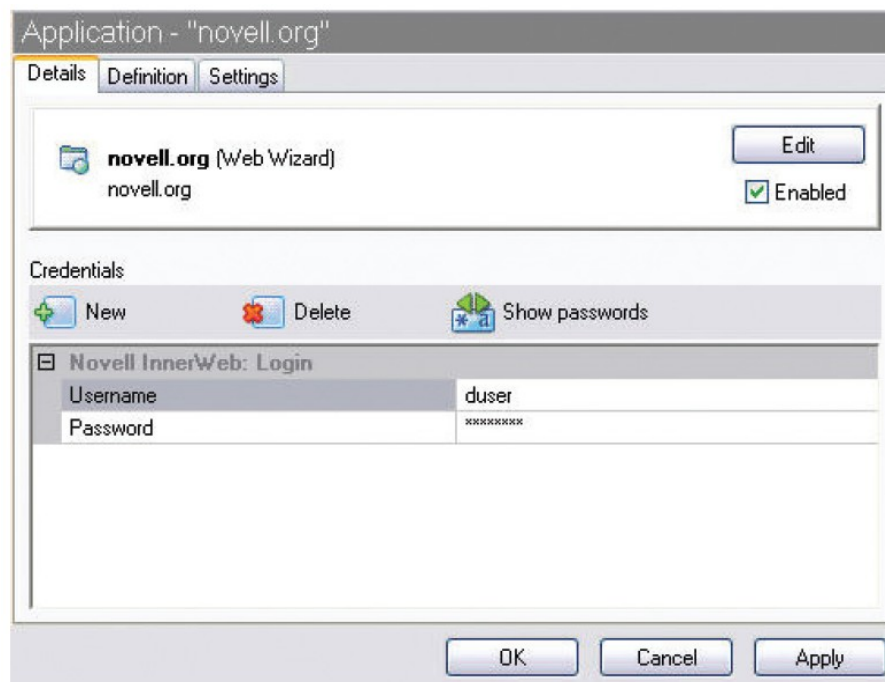
Gdy użytkownicy mają do czynienia ze zbyt dużą liczbą identyfikatorów i haseł, mają skłonność do ich zapisywania lub często je zapominają, a odzyskanie hasła jest stratą czasu zarówno dla użytkownika, jak i pracowników działu IT. Nadmiar haseł jest nie tylko niewygodny, lecz także osłabia poziom bezpieczeństwa. Dlatego przedsiębiorstwo potrzebuje rozwiązania, które wyeliminowałoby frustrację użytkowników związaną z koniecznością pamiętania wielu haseł, zapewniło bezpieczeństwo zasobów korporacyjnych, a także zgodność z coraz większą liczbą wymagań prawnych. Potrzeby te zaspokajają Novell SecureLogin. Rozwiązanie to umożliwia upoważnionym użytkownikom jednokrotne bezpieczne zalogowanie się, które wystarcza do uwierzytelnienia do wszystkich zasobów korporacyjnych, do których dany użytkownik powinien mieć dostęp, takich jak sieć, aplikacje czy zabezpieczone serwisy internetowe. Jednocześnie wyeliminowane zostają kłopoty i koszty związane z obciążaniem helpdesku problemami z resetowaniem zapomnianych haseł.

Cechy i funkcje

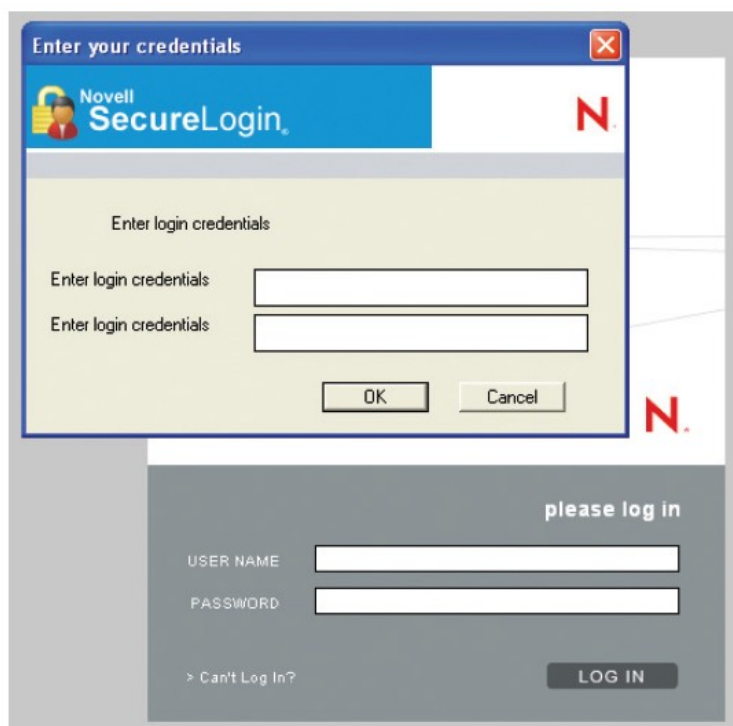
- Umożliwienie użytkownikom jednokrotnego logowania w celu uzyskania dostępu do sieci, poczty elektronicznej, potrzebnych aplikacji, zabezpieczonych stron internetowych itd.
- Obsługa i egzekwowanie wielu złożonych reguł dotyczących haseł
- Prosty interfejs udostępniany pracownikom
- Wykorzystanie katalogu (np. Novell eDirectory lub Active Directory) do scentralizowanej kontroli dostępu, szczegółowego rozróżniania uprawnień oraz zapewnienia elastyczności w obsłudze tożsamości
- Automatyczne konfigurowanie nowych haseł po wygaśnięciu starych
- Obsługa zaawansowanych metod uwierzytelniania, takich jak metody biometryczne, karty procesorowe, karty zbliżeniowe
- Ścisła integracja z systemem zarządzania tożsamością w przedsiębiorstwie w celu automatyzacji czynności związanych z konfigurowaniem kont użytkowników
- Automatyczne, oparte na regułach kontrolowanie komputerów użytkowników, w tym komputerów z systemami Windows Vista i Novell SUSE Linux Enterprise Desktop.



Rys. 1. Przykład działania funkcji jednokrotnego logowania w oprogramowaniu Novell SecureLogin



Rys. 2. Sprawdzanie zapamiętanych identyfikatorów użytkownika i haseł oraz zarządzanie nimi



Rys. 3. Wykrywanie operacji zalogowania

Novell Storage Manager

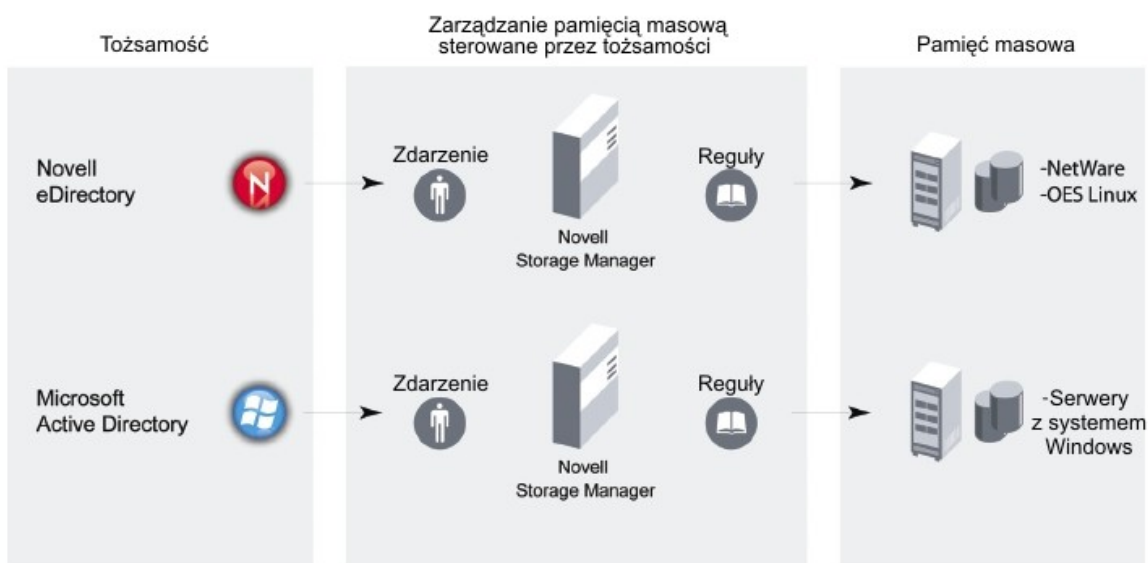
Automatyzacja zarządzania pamięcią masową udostępnioną użytkownikom

Udostępnianie przestrzeni pamięci masowej każdemu użytkownikowi lub grupie użytkowników w sieci, a także zarządzanie tą przestrzenią, nie muszą być utrudnieniem dla działu informatycznego. Stosując oprogramowanie Novell Storage Manager można zautomatyzować udostępnianie pamięci masowej, wyeliminować ręczne, pracochłonne procesy i ograniczyć koszty związane z zarządzaniem pamięcią masową. Novell Storage Manager ułatwia przydzielanie i czyszczenie pamięci masowej oraz zarządzanie nią w oparciu o reguły oraz informacje o tożsamości użytkowników. Rozwiązanie Novella automatyzuje wiele typowych zadań związanych z pamięcią masową, takich jak zarządzanie limitami, zmiana nazw katalogów, migracja, przydzielanie miejsca w zależności od priorytetu oraz archiwizacja.

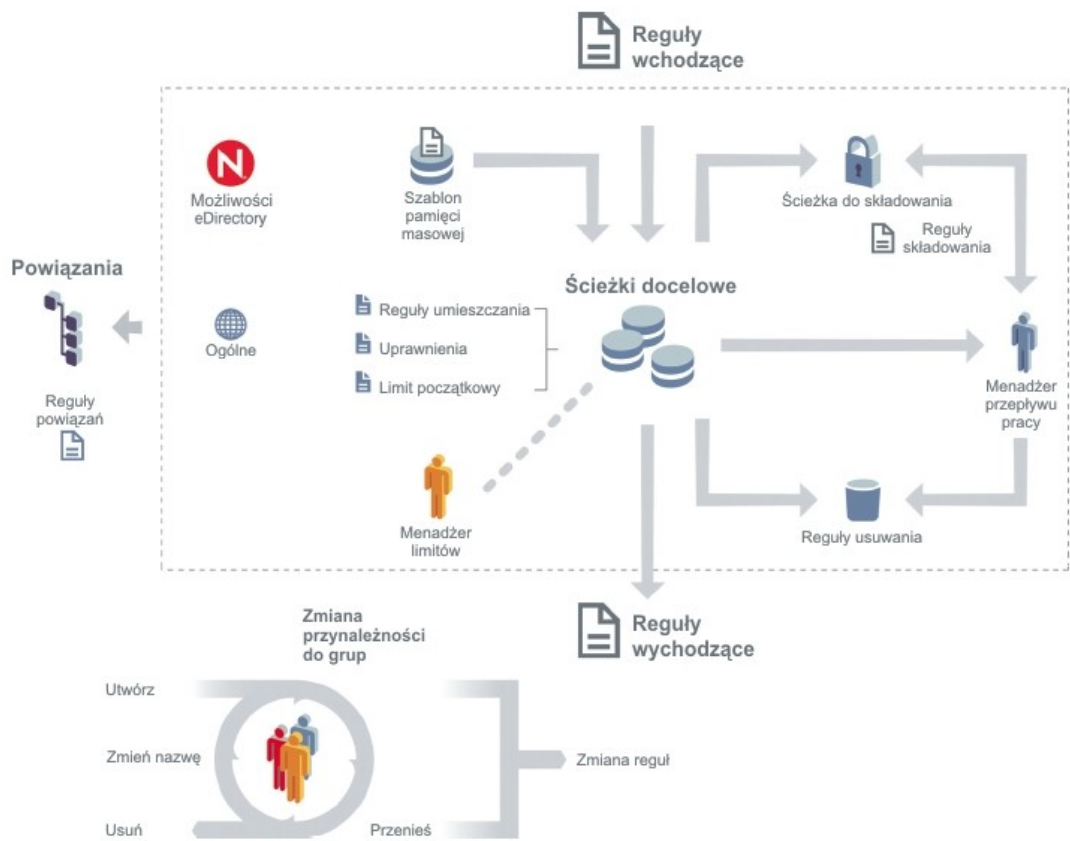
Novell Storage Manager działa na różnych platformach i jest kompatybilny z systemami operacyjnymi Microsoft Windows, Novell Open Enterprise Server w wersji dla SUSE Linux oraz NetWare.

Cechy i funkcje

- Konfigurowanie pamięci masowej i zarządzanie nią w oparciu o tożsamość osoby – rolę pełnioną przez użytkownika w organizacji oraz posiadane przez niego uprawnienia
- Zarządzanie pamięcią masową w oparciu o zdefiniowane reguły jej wykorzystania
- Implementacja reguł usuwania plików i trwałego ich składowania (*vaulting*) dla potrzeb archiwizacji nieaktywnych danych
- Generowanie kompleksowych raportów (np. z informacjami o ostatnim dostępie do pliku, momencie modyfikacji, wielkości, duplikatach plików, typach plików, relacjach zaufania i własności), dotyczących zarówno pamięci masowej poszczególnych użytkowników jak i pamięci wspólnej dla grup użytkowników (np. działu marketingu firmy lub oddziału w Krakowie)
- Moduł analizy uprawnień zapewniający, że tylko właściwi użytkownicy uzyskują uprawnienia dostępu do pamięci masowej
- Automatyzacja migracji danych użytkownika w przypadku zmiany stanowiska lub miejsca pracy
- Egzekwowanie automatycznej, opartej na regułach procedury czyszczenia (lub trwałego składowania) danych po odejściu pracownika z przedsiębiorstwa



Rys. 1. Integracja funkcji związanych z tożsamością i funkcji związanych z pamięcią masową



Rys. 2. Schemat ogólnej stosowania reguł w zarządzaniu pamięcią masową



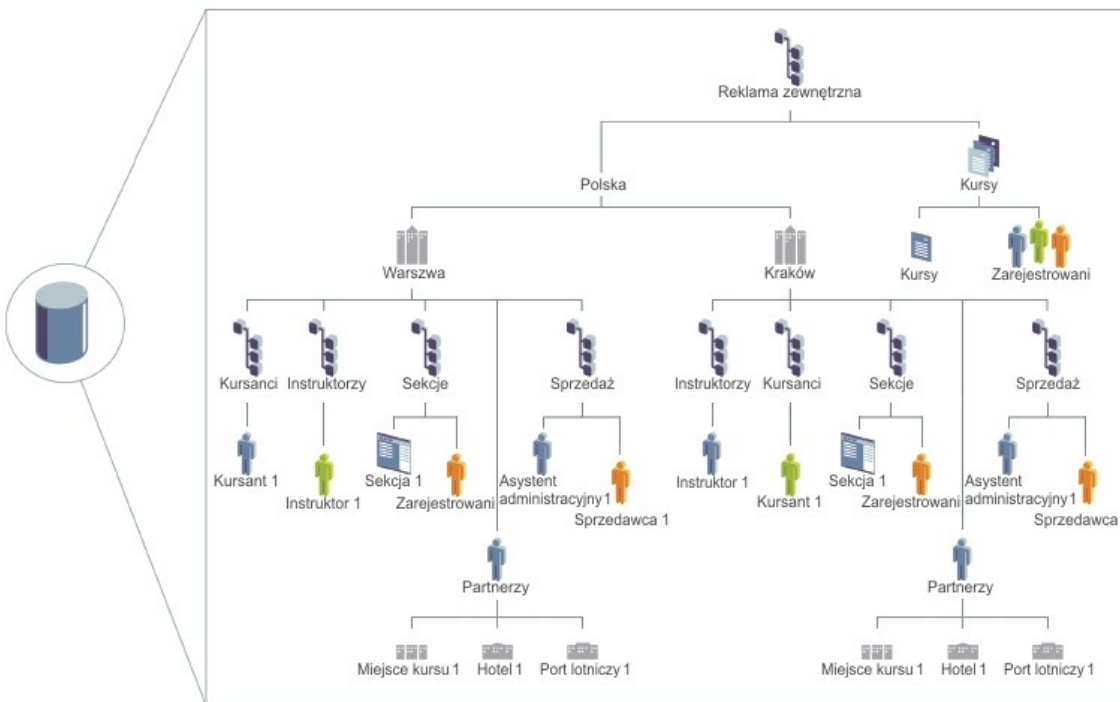
Rys. 3. Zarządzanie pamięcią masową we wszystkich fazach cyklu obsługi użytkownika

Precyzyjna kontrola wszystkich użytkowników i zasobów sieciowych

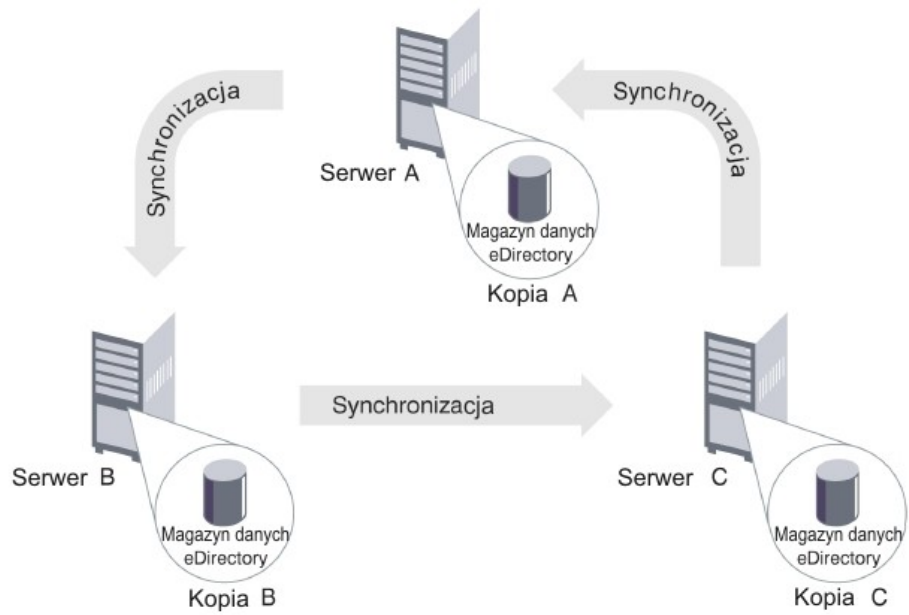
Brak zorganizowanego korzystania z aplikacji, systemów i komputerów użytkowników prowadzi do powtarzania wielu tych samych czynności administracyjnych, straty czasu pracowników IT, niepotrzebnych kosztów. Sprawna organizacja środowiska informatycznego możliwa jest w oparciu o usługi katalogowe, które zapewnią unifikację informacji o tożsamości i uprawnieniach użytkowników, posiadanych zasobach – oprogramowaniu i urządzeniach oraz o obowiązujących regułach. Do najpopularniejszych na świecie usług katalogowych należy Novell eDirectory. Rozwiązanie to cechuje się niezrównaną skalowalnością (obsługa nawet miliardów obiektów w katalogu) i niezawodnością oraz elastyczną, ale zapewniającą wysoki poziom bezpieczeństwa architekturą. System Novell eDirectory jest kompatybilny z najważniejszymi standardami branżowymi i systemami operacyjnymi oraz jest niezwykle łatwy do zarządzania.

Cechy i funkcje

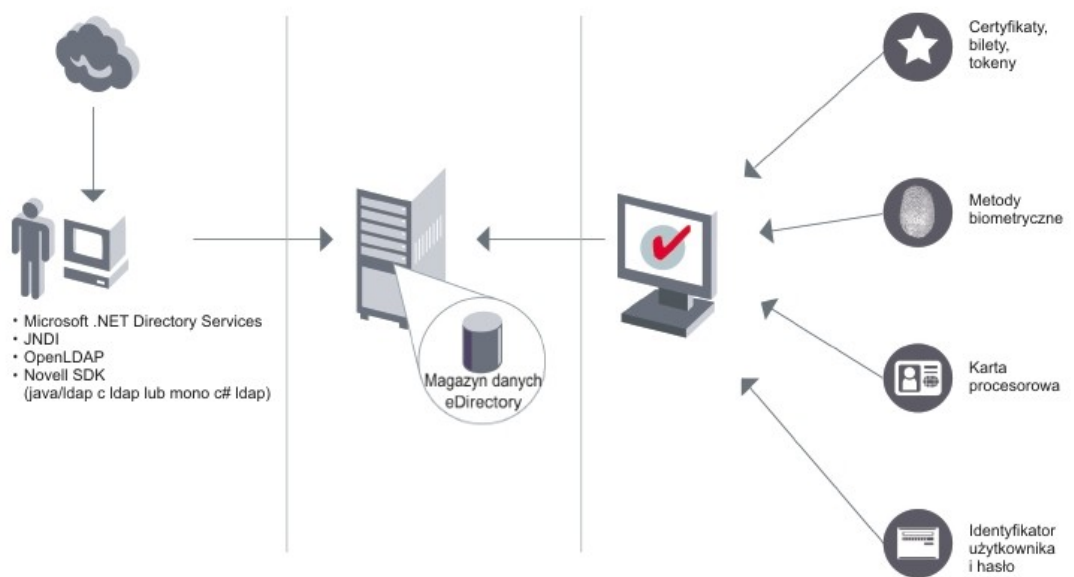
- Skalowanie od wdrożeń najmniejszych do obejmujących ponad miliard tożsamości
- Obsługa standardów otwartych oraz standardów nowo wprowadzanych, w tym LDAP, SOAP, DSML, ADSI i JDBC
- Elastyczna struktura bezpieczeństwa z bezpośrednią obsługą zaawansowanych metod uwierzytelniania
- Przełączanie awaryjne w czasie rzeczywistym i odtwarzanie po awarii
- Kompleksowe narzędzia administracyjne zapewniające elastyczność korzystania z katalogów
- Kompatybilność z systemami Linux, NetWare, Windows, Solaris, AIX i HP-UX
- Opatentowany mechanizm replikacji z wieloma równoprawnymi kopiami, ułatwiający zagwarantowanie dostępu do danych w katalogu np. podczas uwierzytelniania użytkowników.



Rys. 1. Organizowanie zasobów, tożsamości i reguł



Rys. 2. Ochrona danych dzięki automatycznej replikacji



Rys. 3. Interakcja pomiędzy programistą a użytkownikiem



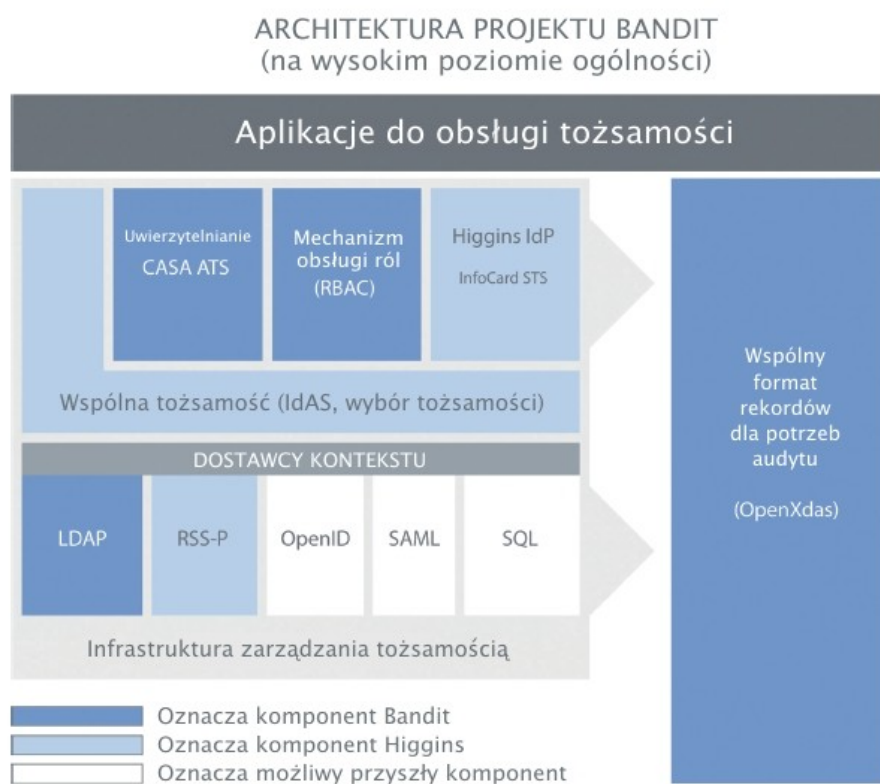
Projekt Bandit

Nowatorskie rozwiązania do zarządzania tożsamością wspierane przez społeczność open source

W miarę jak współczesne przedsiębiorstwa i instytucje coraz szerzej wdrażają technologie zarządzania tożsamością, napotykają na coraz większą, przytłaczającą wręcz liczbę produktów pochodzących od różnych dostawców. Zróżnicowanie tych ofert może stwarzać trudności w integracji systemów i aplikacji wykorzystujących często te same informacje o tożsamości. W celu wyjścia naprzeciw tym problemom Novell zainicjował projekt pod nazwą Bandit wspierany przez społeczność open-source. Celem projektu jest ujednoczenie zróżnicowanych systemów zarządzania tożsamością oraz wprowadzenie spójnego podejścia do zabezpieczenia tożsamości i zarządzania tożsamością. W skład projektu wchodzi dużo powiązane komponenty typu open source (z otwartym dostępem do kodu źródłowego), które udostępniają jednolite usługi zarządzania tożsamością, obejmujące uwierzytelnianie, autoryzację i audyt. Komponenty te implementują protokoły i specyfikacje oparte na otwartych standardach, co oznacza, że usługi zarządzania tożsamością mogą być tworzone, używane, integrowane i oparte na wielu źródłach tożsamości.

Cechy i funkcje

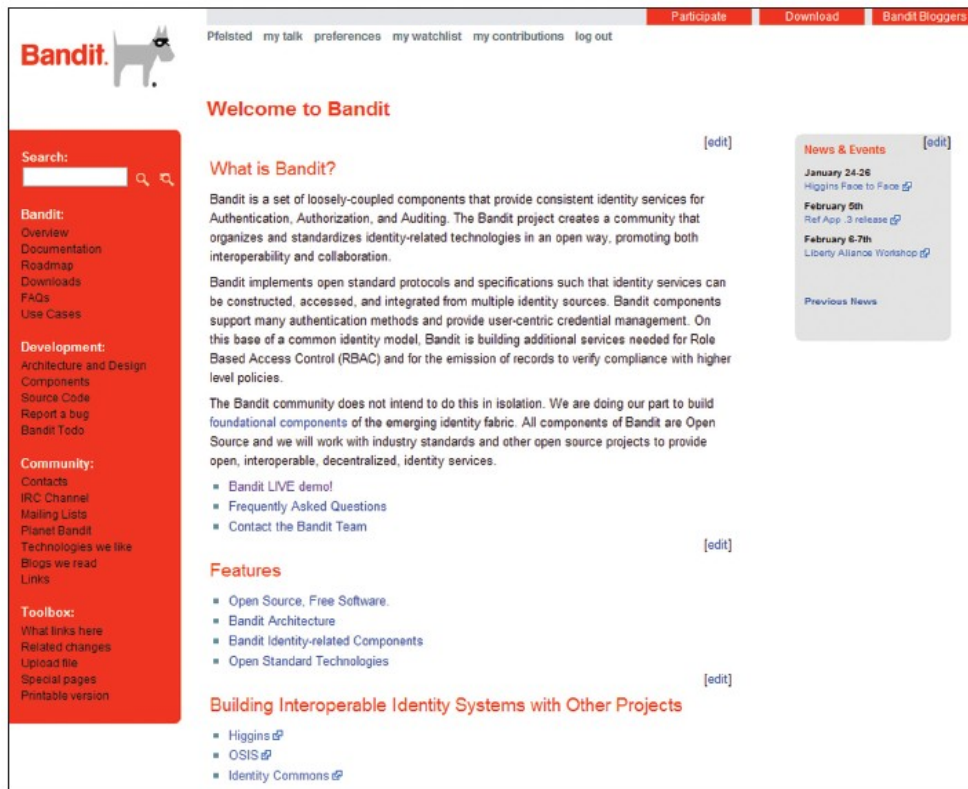
- Prosty dostęp z aplikacji do wielu magazynów z danymi o tożsamościach
- Obsługa wielu metod uwierzytelniania (w tym dołączanych jako wtyczki) przy zapewnieniu jednolitego dostępu do aplikacji
- Prosty interfejs aplikacji zapewniający jednolity dostęp do systemów w oparciu o role
- Łatwe włączanie aplikacji do wspólnego systemu zapewnienia zgodności z przepisami



Rys. 1. Schemat ogólnej architektury



Rys. 2. Praca z aplikacją Microsoft CardSpace



Rys. 3. Strona główna projektu Bandit: www.bandit-project.org

Informacje kontaktowe

Więcej informacji o rozwiązaniach firmy Novell do zarządzania tożsamością i bezpieczeństwem można uzyskać kontaktując się z biurem Novell Polska lub na stronie internetowej www.novell.com/management

Novell Polska Sp. z o.o.

ul. Wspólna 47/49

00-684 Warszawa

tel. 0 22 537 5000

bezpłatna infolinia 0 800 22 66 85

infolinia@novell.pl

INFORMACJE O FIRMIE NOVELL

Novell dostarcza światowej klasy oprogramowanie i usługi oparte na produktach open source i technologiach komercyjnych wykorzystujących otwarte standardy. Pomagamy klientom w zarządzaniu, upraszczaniu, zabezpieczaniu i integrowaniu systemów informatycznych w celu obniżania stopnia złożoności i kosztów posiadania infrastruktury IT. Oferujemy ponadto szkolenia i wsparcie techniczne.

Więcej informacji: www.novell.com

464-001008-003 | 05/07 | © 2007 Novell Inc. Wszelkie prawa zastrzeżone. Novell, logo Novell, logo „N”, GroupWise, NDS i NetWare są zastrzeżonymi znakami towarowymi, zaś Bandit, 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.