

Novell Identity Manager 4.0 Advanced Edition

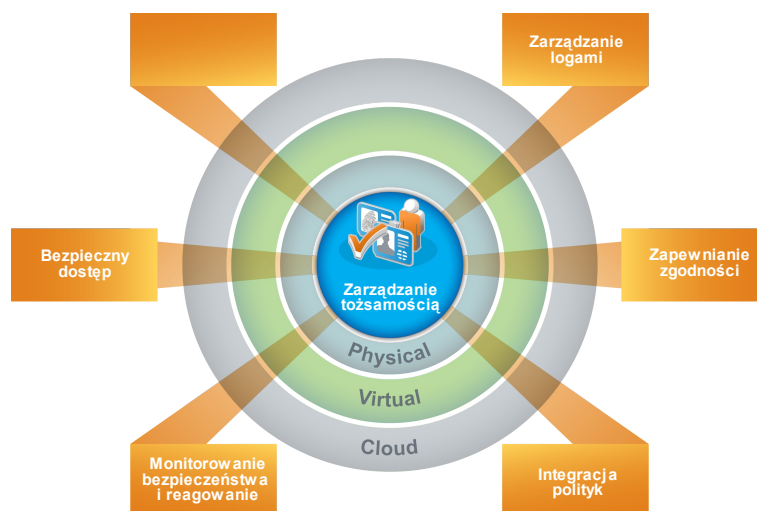
Zarządzanie tożsamością i dostępem w środowiskach fizycznych,
wirtualnych oraz środowiskach typu cloud

Novell.

Novell Identity Manager 4.0 Advanced Edition

Novell Identity Manager 4.0 Advanced Edition bezpiecznie zarządza tożsamością i udostępnianiem zasobów w środowiskach fizycznych, wirtualnych oraz środowiskach typu cloud z użyciem inteligentnego mechanizmu tożsamości, umożliwiającego wykorzystanie istniejących zasobów informatycznych oraz nowych modeli takich jak SaaS przy jednoczesnym obniżeniu kosztów i zapewnieniu zgodności z wymogami przepisów. Zapewnia istotne korzyści we wszystkich aspektach działania firmy, doceniane przez menedżerów różnych działów, np.:

- Ułatwia **dyrektorom informatyki** zwiększanie produktywności dzięki uproszczeniu administrowania i zaawansowanym mechanizmom raportowania przy zapewnieniu skutecznej kontroli poziomów jakości usług, co umożliwia lepsze wykorzystywanie nowych możliwości.
- Pozwala **szefom bezpieczeństwa** w ekonomiczny sposób gwarantować zgodność z wymogami przepisów i bezpieczeństwo zasobów informatycznych w środowiskach fizycznych, wirtualnych i środowiskach typu cloud.
- Umożliwia **menedżerom biznesowym** (LoB) utrzymanie wysokiej produktywności pracowników przez zapewnienie im dostępu do zasobów adekwatnego do ich ról oraz mechanizmu samoobsługi z wygodnym i łatwym w użyciu interfejsem.
- Pozwala **menedżerom informatyki** osiągnąć więcej z wykorzystaniem posiadanych zasobów dzięki rozbudowanej automatyzacji – od sprawnej obsługi wezwań serwisowych po realizację wymagań przepisów.



Nowości i usprawnienia w wydaniu Novell Identity Manager 4.0 Advanced Edition obejmują:

- **Udostępnianie zasobów w oparciu o role:** Najbardziej efektywne rozwiązanie do udostępniania zasobów ze zintegrowanymi mechanizmami obsługi ról i reguł oraz przekazywania zadań (*workflow*) – wyposażone w przyjazny interfejsem użytkownika.
- **Zaawansowane raportowanie:** Kompleksowe funkcje raportowania stanów aktualnych i historycznych w infrastrukturach klasycznych i typu cloud z możliwością tworzenia niestandardowych raportów.
- **Udostępnianie zasobów w środowiskach typu cloud:** Gotowe konektory rozszerzające istniejące polityki na aplikacje SaaS (np. Salesforce.com).
- **Integracja polityk:** Administrator ds. mapowania ról, zdolny wykrywać autoryzacje w obrębie systemów informatycznych i integrować je z rolami pełnionym przez pracowników firmy, tworząc jednolite polityki.
- **Zarządzanie treścią:** Menedżer pakietów, upraszczający tworzenie, dystrybucję i wykorzystanie wysokiej jakości elementów treści do budowy modułowych polityk.
- **Uproszczona instalacja i wdrożenie:** Zintegrowany instalator oraz inteligentne narzędzia wdrożeniowe, takie jak Designer i Analityk, automatyzujące proces wdrożenia.
- **Interfejsy oparte na standardach:** Ponad 100 usług gotowych do obsługi tożsamości dostępnych za pośrednictwem interfejsów REST i SOAP ułatwia integrację w istniejących środowiskach.

Identity Manager i automatyzacja procesów biznesowych

Niniejsza broszura pokazuje, jakie problemy biznesowe pomaga rozwiązywać Novell Identity Manager 4.0 Advanced Edition, pozwalając jednocześnie obniżyć koszty i zagwarantować zgodność z wymogami przepisów. Zawiera ona również opis techniczny elementów Identity Manager oraz narzędzi, za pomocą których można stworzyć własne wdrożenie Identity Manager.

Informacje zawarte w tym rozdziale wskazują niektóre procesy biznesowe, które można zautomatyzować dzięki implementacji systemu Novell Identity Manager. Zarządzanie tożsamością należy do podstawowych czynności w większości firm. Wyobraźmy sobie sytuację w poniedziałkowy poranek. Oto lista zgłoszeń:

- Zmienił się numer telefonu Jerzego Talara. Należy go zaktualizować w bazie danych kadr i czterech innych, niezależnych systemach.
- Katarzyna Hańcza po powrocie z długiego zwolnienia nie pamięta hasła do swej poczty. Trzeba jej pomóc je odtworzyć lub zresetować.
- Jan Graś zatrudnił nowego pracownika. Trzeba mu zapewnić dostęp do sieci i utworzyć konto pocztowe.
- Inga Biernacka prosi o dostęp do bazy finansowej Oracle, co wymaga od ciebie uzyskania zgody trzech menedżerów.
- Marcin Rosiński przeniósł się z działu finansowego do prawnego. Należy przydzielić mu dostęp do tych samych zasobów, jak w przypadku innych członków zespołu prawnego i odebrać dostęp do zasobów działu finansowego.
- Jarosław Nowak, twój szef, zobaczył wniosek Ingi Biernackiej o dostęp do bazy finansowej Oracle i jest zaniepokojony liczbą osób mających do niej dostęp. Prosi o sporządzenie raportu ukazującego wszystkie osoby mające dostęp do tej bazy.

Bierzesz głęboki wdech i zaczynasz od pierwszego zgłoszenia, wiedząc, że będzie trudno zdążyć z realizacją wszystkich, nie mówiąc już o pozostałych projektach, które ci powierzono.

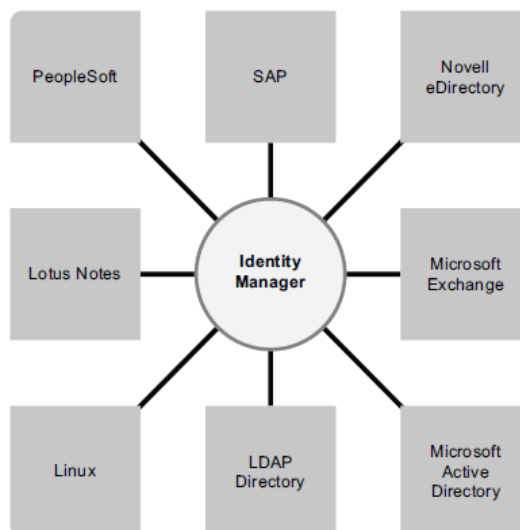
Jeśli powyższa sytuacja przypomina typowy dzień na miejscu pracy twoim lub kogoś w twojej firmie, Identity Manager może się okazać pomocny. Podstawowe mechanizmy Identity Managera, ukazane na poniższej ilustracji, pozwalają zautomatyzować wszystkie wspomniane czynności – i nie tylko. Owe mechanizmy – przekazywanie zadań, role, poświadczenie, samoobsługa, audytowanie i raportowanie – wykorzystują wielosystemową synchronizację danych zgodnie z ustalonymi politykami, automatyzując procesy związane z udostępnianiem zasobów i zarządzaniem hasłami, które należą do najtrudniejszych i najbardziej pracochłonnych zadań działów informatyki.



Rys. 1 Podstawowe mechanizmy Identity Managera

Synchronizacja danych

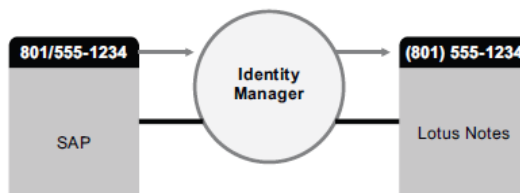
W większości firm dane o tożsamości przechowywane są w wielu systemach albo w jednym, który może być wykorzystywany przez inne systemy. Tak czy inaczej, konieczna jest możliwość łatwego współdzielenia i synchronizacji danych między systemami. Identity Manager pozwala synchronizować, przekształcać i przekazywać informacje między szeroką gamą aplikacji, baz danych, systemów operacyjnych i katalogów takich jak SAP, PeopleSoft, Salesforce, Microsoft SharePoint, Lotus Notes, Microsoft Exchange, Microsoft Active Directory, Novell eDirectory, Linux, UNIX i katalogi LDAP.



Rys. 2 Novell Identity Manager łączy różnorodne systemy

Novell Identity Manager 4.0 Advanced Edition zapewnia kontrolę nad przepływem danych między połączonymi systemami – między innymi określanie, jakie dane mają być współdzielone, który system jest autorytatywnym źródłem danych i w jaki sposób dane mają być interpretowane i przekształcane, by spełniać wymagania innych systemów.

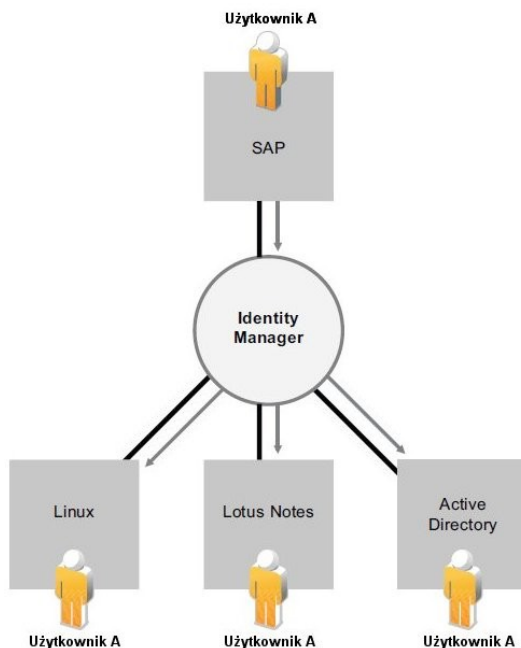
Na poniższej ilustracji, baza danych kadrowych SAP jest autorytatywnym źródłem numeru telefonu użytkownika. System Lotus Notes również używa numerów telefonów, więc Identity Manager przekształca numer na wymagany format i udostępnia go systemowi Lotus Notes. Jeśli numer zmienia się w bazie SAP, jest synchronizowany z systemem Lotus Notes.



Rys. 3 Synchronizacja danych między połączonymi systemami

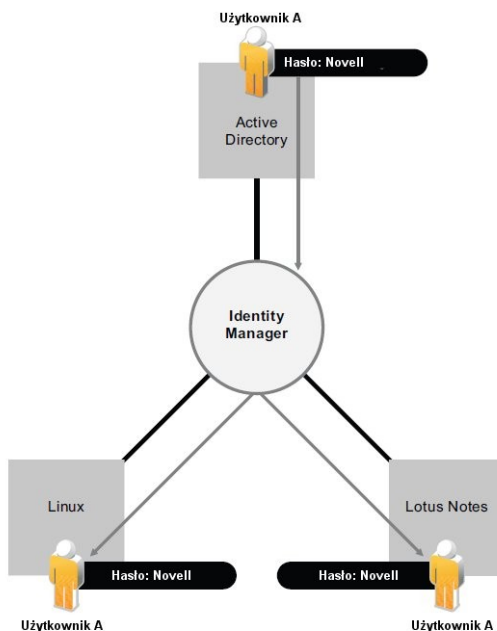
Zarządzanie danymi istniejących użytkowników to tylko początek możliwości systemu Novell Identity Manager 4.0 Advanced Edition w zakresie synchronizacji danych. Identity Manager może również tworzyć nowe konta użytkowników i usuwać istniejące konta w katalogach (np. Active Directory), systemach biznesowych i pocztowych (SAP, PeopleSoft; Lotus Notes, Exchange) i systemach operacyjnych, jak UNIX czy Linux.

Jeśli na przykład do systemu kadrowego SAP zostaje dodany nowy pracownik, Identity Manager może automatycznie utworzyć nowe konta użytkownika w Active Directory, Lotus Notes oraz w systemie zarządzania kontami Linux NIS.



Rys. 4 Tworzenie kont użytkowników w połączonych systemach

Funkcje synchronizacji danych w systemie Novell Identity Manager 4.0 Advanced Edition pozwalają także synchronizować hasła między systemami. Jeśli na przykład użytkownik zmienia swoje hasło w Active Directory, Identity Manager może dokonać jego synchronizacji w systemach Lotus Notes i Linux.

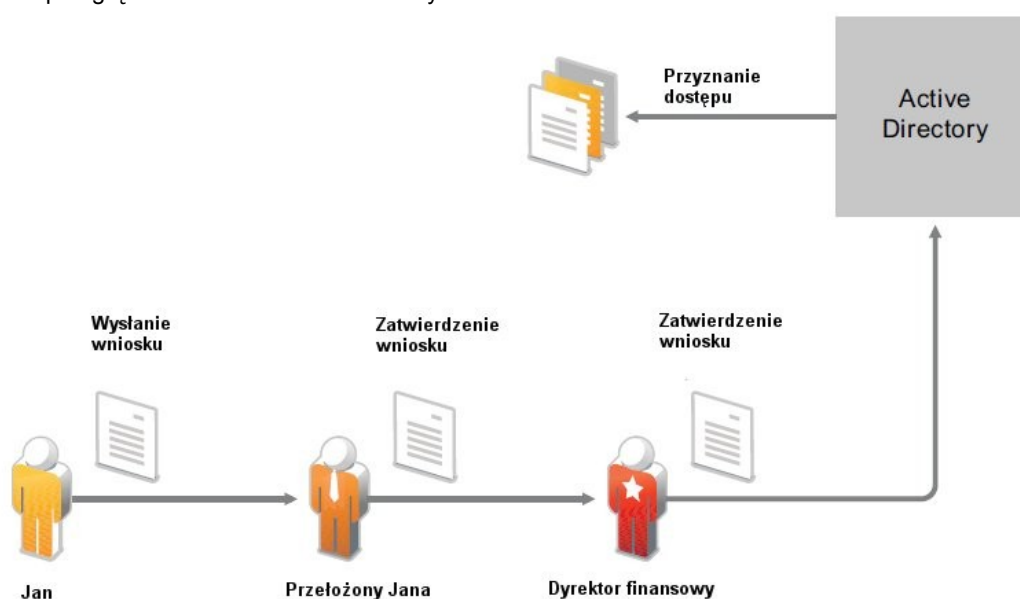


Rys. 5 Synchronizacja haseł w połączonych systemach

Przekazywanie zadań

Często dostęp użytkowników do wielu zasobów w firmie nie wymaga niczyjej akceptacji. Jednakże dostęp do niektórych zasobów może być ograniczony i wymagać akceptacji jednej lub kilku osób.

Novell Identity Manager 4.0 Advanced Edition udostępnia mechanizmy przekazywania zadań, które gwarantują, że proces przydzielania dostępu do zasobów będzie uwzględniał akceptacje określonych osób. Załóżmy na przykład, że Jan, któremu przydzielono już konto Active Directory, wnioskuje o dostęp do pewnych raportów finansowych za pośrednictwem Active Directory. Wymaga to akceptacji zarówno bezpośredniego przełożonego Jana, jak i dyrektora finansowego. Na szczęście utworzony wcześniej schemat przekazywania zadań przekazuje wniosek Jana do jego przełożonego, a po jego akceptacji – do dyrektora finansowego, którego zgoda powoduje automatyczne przyznanie praw dostępu Active Directory, potrzebnych Janowi do przeglądania dokumentów finansowych.



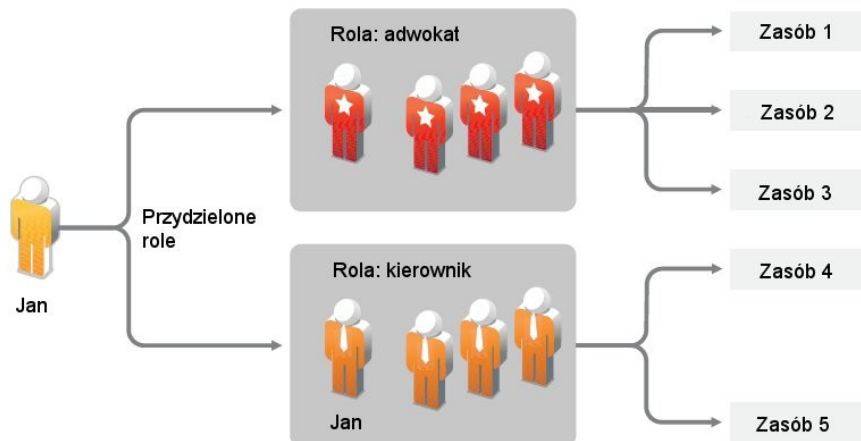
Rys. 6 Przekazywanie wniosku o udostępnienie zasobów

Przekazywanie zadań może być inicjowane automatycznie po wystąpieniu określonego zdarzenia (na przykład, gdy do systemu kadrowego zostanie dodany nowy użytkownik) lub manualnie, poprzez wniosek użytkownika. Dla zapewnienia szybkiego przyznawania (lub nie) dostępu można definiować pełnomocników oraz grupy osób upoważnionych do akceptowania wniosków.

Role i poświadczenie

Użytkownicy często potrzebują dostępu do zasobów związanych z rolą pełnioną przez nich w firmie. Na przykład w firmie prawniczej adwokaci mogą mieć dostęp do innych zasobów, niż ich asystenci. Novell Identity Manager 4.0 Advanced Edition pozwala udostępniać zasoby w oparciu o role użytkowników. Można więc definiować role i przypisywać im uprawnienia zgodnie z potrzebami firmy. Gdy dany użytkownik ma przypisaną określoną rolę, Identity Manager udostępnia mu zasoby przypisane do tej roli.

Jeśli użytkownik ma przypisanych kilka ról, uzyskuje dostęp do zasobów przypisanych do tych ról, jak na poniższej ilustracji:



Rys. 7 Udostępnianie zasobów w oparciu o role

Role mogą być przypisywane użytkownikom automatycznie w efekcie określonych zdarzeń (na przykład do bazy kadrowej SAP zostaje dodany nowy użytkownik o stanowisku adwokata). Jeśli przypisanie roli wymaga akceptacji, można zdefiniować przekazywanie zadań, kierujące wnioskiem o akceptację do odpowiedniej osoby. Można również przypisywać role manualnie.

W pewnych przypadkach określone role nie mogą być łączone przez tę samą osobę ze względu na konflikt ról. Novell Identity Manager 4.0 Advanced Edition udostępnia funkcję rozdzielania obowiązków, która zapobiega przypisaniu użytkownikowi konfliktowych ról, chyba, że odpowiednia osoba uczyni w tej sprawie wyjątek.

Ponieważ przypisane role decydują o dostępie użytkownika do zasobów, zapewnienie właściwego przypisania ma znaczenie nieważne. Niewłaściwe przypisania mogłyby zagrozić zgodności z wymogami przepisów, czy regulacji wewnętrznych bądź państwowych. Novell Identity Manager 4.0 Advanced Edition pozwala weryfikować poprawność przypisania ról za pomocą procesu poświadczania.

Korzystając z tego procesu, odpowiedzialne osoby certyfikują dane powiązane z rolami:

- **Poświadczenie profilu użytkownika:** wybrani użytkownicy poświadczają informacje zawarte w swoim profilu (imię, nazwisko, tytuł, wydział, adres e-mail itd.) i poprawiają nieprawidłowe informacje. Rzetelność informacji zawartych w profilu jest kluczowa dla prawidłowego przypisania ról.
- **Poświadczenie rozdzielania obowiązków:** Odpowiedzialne osoby weryfikują raport o naruszeniu rozdzielania obowiązków i poświadczają jego rzetelność. Raport ten wylicza ewentualne wyjątki, umożliwiające przypisanie użytkownikowi konfliktowych ról.
- **Poświadczenie przypisania roli:** Odpowiedzialne osoby weryfikują raport wyliczający wybrane role oraz użytkowników, grupy oraz uprawnienia przypisane do każdej z ról i poświadczają rzetelność informacji.
- **Poświadczenie przypisania użytkownika:** Odpowiedzialne osoby weryfikują raport wyliczający wybranych użytkowników oraz przypisane im role i poświadczają rzetelność informacji.

Owe raporty i poświadczenia mają na celu zagwarantowanie prawidłowości przypisania ról oraz istnienie istotnych przyczyn uzasadniających wyjątki przy przypisaniu konfliktowych ról.

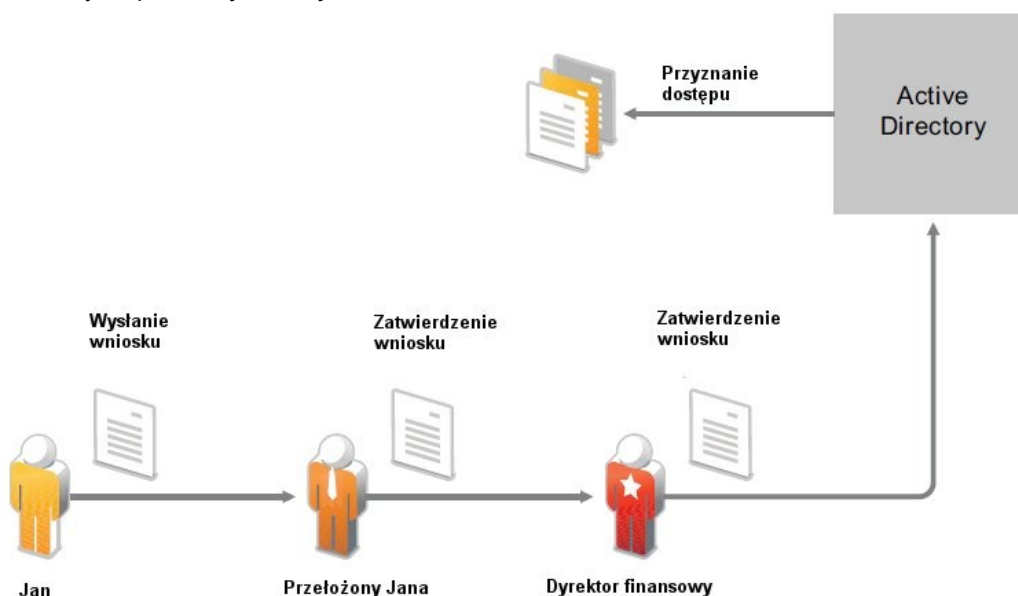
Samoobsługa

Zwykle każdy dział IT ma do czynienia z menedżerami czy działami w firmie domagającymi się możliwości samodzielnego zarządzania informacjami o swoich użytkownikach i ich uprawnieniach, bez konieczności korzystania z usług administratorów. Często słyszy się pretensje w rodzaju: „Dlaczego nie mogę zmienić swojego numeru telefonu w bazie kontaktów?”, czy też: „Pracuję w dziale marketingu. Czemu muszę prosić administratora o możliwość dostępu do bazy danych marketingowych?”

Korzystając z Identity Managera, można delegować obowiązki administratora na osoby, które będą za nie odpowiedzialne. Można na przykład pozwolić określonemu użytkownikowi na:

- **Zarządzanie danymi osobistymi w bazie kontaktów.** Zamiast prosić dział IT o zmianę numeru telefonu, można samemu zmienić go w jednym miejscu, a Identity Manager dokona synchronizacji we wszystkich systemach.
- **Zmianę haseł, ustawienie podpowiedzi oraz pytań i odpowiedzi dla zapomnianych haseł.** Zamiast prosić dział IT o zresetowanie zapomnianego hasła, można skorzystać z podpowiedzi lub zresetować je samodzielnie, udzielając prawidłowo odpowiedzi na zdefiniowane wcześniej pytania.
- **Uzyskać dostęp do zasobów takich, jak bazy danych, systemy czy katalogi.** Zamiast prosić dział IT o przyznanie dostępu do aplikacji, można samodzielnie wybrać ją z listy dostępnych zasobów.

Oprócz mechanizmu samoobsługi dla użytkowników, Novell Identity Manager 4.0 Advanced Edition umożliwia samoobsługową administrację dla funkcji odpowiedzialnych za asystę, monitorowanie i akceptację wniosków użytkowników (np. pomoc techniczna). Weźmy na przykład raz jeszcze scenariusz z opisu przekazywania zadań, ukazany na poniższej ilustracji.



Rys. 8 Przekazywanie wniosku o udostępnienie zasobów z samoobsługą

Nie tylko Jan używa mechanizmu samoobsługi Identity Managera, by złożyć wniosek o dostęp do potrzebnych mu dokumentów, ale i jego przełożony i dyrektor finansowy korzystają z mechanizmu samoobsługi do akceptacji wniosku. Zdefiniowany schemat przekazywania danych pozwala Janowi zainicjować i monitorować realizację jego wniosku, zaś jego przełożonemu i dyrektorowi finansowemu – odpowiedzieć na ten wniosek. Akceptacja wniosku przez przełożonego Jana i dyrektora finansowego uruchamia przyznanie praw Active Directory, niezbędnych Janowi do przeglądania dokumentów finansowych.

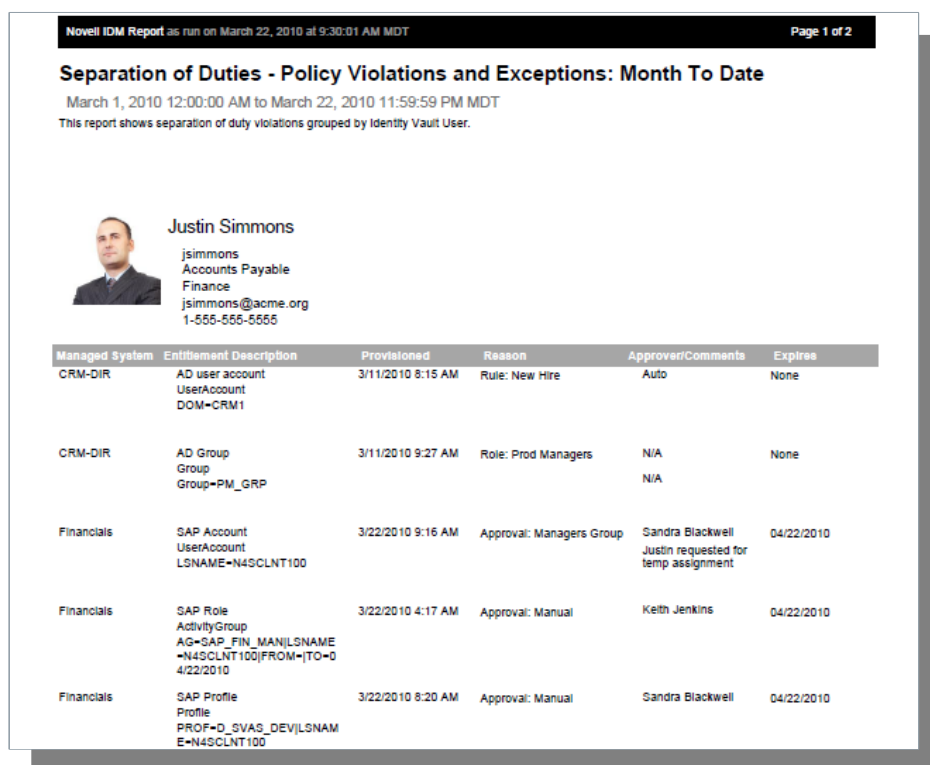
Audytowanie, raportowanie i zapewnianie zgodności z przepisami

Udostępnianie zasobów bez Identity Managera może być nużącym, czasochłonnym i kosztownym wysiłkiem. Wysiłek ten okazuje się jednak mały w porównaniu z tym, który trzeba byłoby włożyć nie posiadając Identity Managera w weryfikowanie zgodności tych działań z politykami firmy, wymogami i regulacjami prawnymi. Czy właściwe osoby mają dostęp do właściwych zasobów? Czy określone zasoby są zabezpieczone przed dostępem niepowołanych osób? Czy zatrudniony właśnie pracownik ma dostęp do sieci, poczty elektronicznej i sześciu innych systemów, niezbędnych mu do pracy? Czy pracownikowi zwolnionemu w zeszłym tygodniu zostały odebrane prawa dostępu?

Dzięki systemowi Novell Identity Manager 4.0 Advanced Edition można mieć pewność, że wszystkie historyczne i obecne działania związane z udostępnianiem zasobów są śledzone i rejestrowane na potrzeby audytów. Identity Manager zawiera inteligentne repozytorium informacji o rzeczywistym i pożądanym stanie rejestru tożsamości i zarządzanych systemach. Za pomocą odpowiednich zapytań uzyskuje się wszelkie informacje dające pewność się, że firma pozostaje w zgodności z wymogami prawa i przepisów.

Zgromadzone informacje dają pełny obraz uprawnień biznesowych, dostarczając wiedzy o przeszłym i obecnym stanie autoryzacji i pozwoleń udzielonych osobom (tożsamościom) w firmie. Dysponując tą wiedzą, można odpowiedzieć nawet na najbardziej wyrafinowane zapytania w kwestiach nadzoru nad przedsiębiorstwem, ograniczania ryzyka i zgodności z wymogami przepisów.


Novell Identity Manager 4.0 Advanced Edition zawiera wstępnie zdefiniowane raporty, pozwalające wysłać zapytania do hurtowni informacji o tożsamości (Identity Information Warehouse) w celu wykazania zgodności z politykami w obszarze biznesowym, informatycznym i korporacyjnym. Można również tworzyć własne raporty, jeśli gotowe raporty nie spełniają specyficznych potrzeb firmy.



Novell IDM Report as run on March 22, 2010 at 9:30:01 AM MDT Page 1 of 2

Separation of Duties - Policy Violations and Exceptions: Month To Date

March 1, 2010 12:00:00 AM to March 22, 2010 11:59:59 PM MDT
This report shows separation of duty violations grouped by Identity Vault User.

 Justin Simmons
jsimmons
Accounts Payable
Finance
jsimmons@acme.org
1-555-555-5555

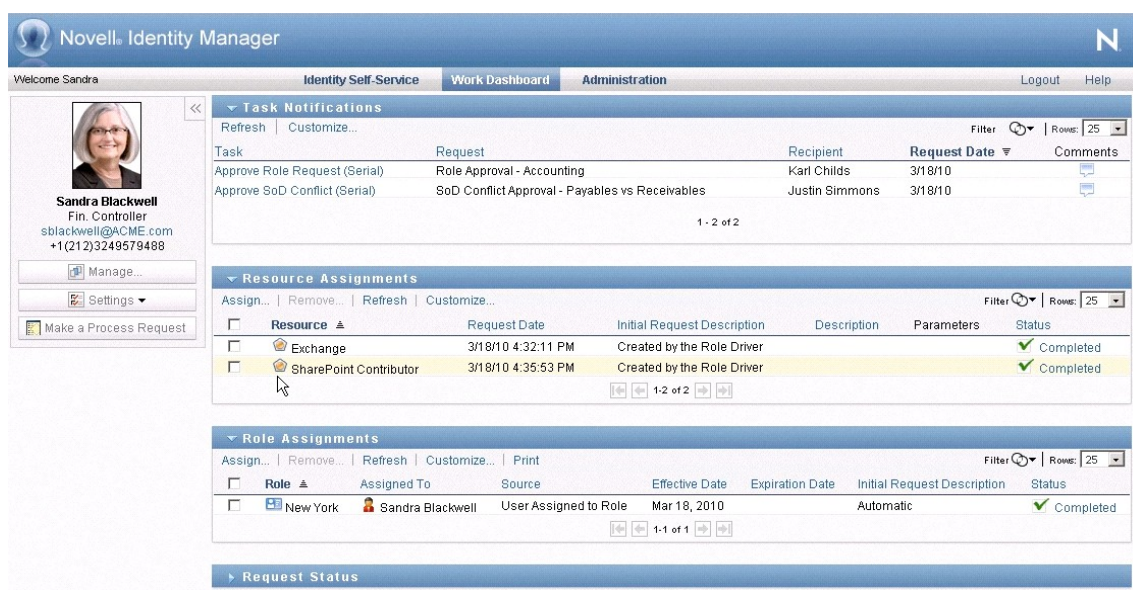
Managed System	Entitlement Description	Provisioned	Reason	Approver/Comments	Expires
CRM-DIR	AD user account UserAccount DOM=CRM1	3/11/2010 8:15 AM	Rule: New Hire	Auto	None
CRM-DIR	AD Group Group Group=PM_GRP	3/11/2010 9:27 AM	Role: Prod Managers	N/A N/A	None
Financials	SAP Account UserAccount LSNAME=N4SCLNT100	3/22/2010 9:16 AM	Approval: Managers Group	Sandra Blackwell Justin requested for temp assignment	04/22/2010
Financials	SAP Role ActivityGroup AG=SAP_FIN_MAN LSNAME =N4SCLNT100 FROM= TO=0 4/22/2010	3/22/2010 4:17 AM	Approval: Manual	Keith Jenkins	04/22/2010
Financials	SAP Profile Profile PROF=D_SVAS_DEV LSNAM E=N4SCLNT100	3/22/2010 8:20 AM	Approval: Manual	Sandra Blackwell	04/22/2010

Rys. 9 Identity Manager raportuje szczegółowo informacje o każdej tożsamości i jej uprawnieniach

Charakterystyka systemu

Novell Identity Manager 4.0 Advanced Edition udostępnia inteligentną infrastrukturę do obsługi tożsamości, pozwalającą wykorzystać istniejące zasoby informatyczne oraz nowe modele przetwarzania, takie jak SaaS (Software as a Service), zapewniając obniżenie kosztów i gwarantując zachowanie zgodności z wymogami przepisów w środowiskach fizycznych, wirtualnych i środowiskach typu cloud. Korzystając z rozwiązań Novell Identity Manager można mieć pewność, że firma dysponuje najbardziej aktualnymi informacjami o tożsamości użytkowników. Możliwość zarządzania tożsamością, udostępniania zasobów i odbierania dostępu zarówno za zaporą (*firewall*), jak i w chmurze, oznacza zachowanie kontroli na poziomie korporacyjnym. Identity Manager pozwala także rozciągnąć zarządzanie zgodnością z wymogami przepisów na środowiska typu cloud.

Novell Identity Manager 4.0 Advanced Edition oferuje możliwość zintegrowanego zarządzania tożsamością i rolami, zaawansowane funkcje raportowania oraz zarządzania pakietami w celu wstępnej konfiguracji i dostosowywania polityk sterujących w systemie Identity Manager. Można również egzekwować polityki bezpieczeństwa, obejmując nimi różnorodne systemy. Rozwiązanie umożliwia zarządzanie pełnym cyklem obecności użytkownika w firmie (od zatrudnienia po zwolnienie) z uwzględnieniem narastających wymagań przepisów. Identity Manager stosuje precyzyjne mechanizmy ochrony z uwagi na przemyślane konfigurowanie kont użytkowników w celu zaspokojenia ich potrzeb jak i spełnienia coraz ostrzejszych wymogów bezpieczeństwa. Inteligentna infrastruktura tożsamości pozwala wykorzystać istniejące zasoby informatyczne z nowymi modelami przetwarzania, takimi jak SaaS.



The screenshot displays the Novell Identity Manager interface for user Sandra Blackwell. The interface is divided into several sections:

- Task Notifications:** A table showing pending tasks. Two tasks are listed: 'Approve Role Request (Serial)' for 'Role Approval - Accounting' and 'Approve SoD Conflict (Serial)' for 'SoD Conflict Approval - Payables vs Receivables'. Both tasks are assigned to 'Karl Childs' and 'Justin Simmons' respectively, with a request date of 3/18/10.
- Resource Assignments:** A table showing assigned resources. Two resources are listed: 'Exchange' and 'SharePoint Contributor'. Both were assigned on 3/18/10 and are marked as 'Completed'.
- Role Assignments:** A table showing assigned roles. One role is listed: 'New York', assigned to 'Sandra Blackwell' on 3/18/10, with an expiration date of 'Mar 18, 2010' and a status of 'Completed'.

Rys. 10 Interfejs systemu Identity Manager precyzyjnie pokazuje wszystkie funkcje pełnione przez daną osobę w organizacji, przyznane uprawnienia jak i zadania zawiązane z przydzielaniem dostępu.

Novell Identity Manager 4.0 Advanced Edition – rozwiązanie całościowe

- **Kompleksowe, gotowe do użycia mechanizmy raportowania:** Zintegrowany moduł raportowania zawarty w pakiecie Novell Identity Manager 4.0 Advanced Edition zapewnia lepszą świadomość zgodności z przepisami zarówno w środowiskach lokalnych, jak i środowiskach typu cloud. Nowe funkcje raportowania pozwalają przeglądać stan tożsamości użytkowników oraz prawa dostępu, a także sporządzać raporty działań użytkowników i historii udostępniania zasobów.

- **Lepsza integracja:** W przypadku nowych wdrożeń systemu Identity Manager, w których wszystkie elementy znajdują się na tym samym serwerze, zintegrowany instalator Novell Identity Manager 4.0 Advanced Edition upraszcza proces instalacji i pozwala szybciej skonfigurować system. Zamiast instalować każdy z komponentów Identity Managera oddzielnie, korzystając ze zintegrowanego instalatora można zainstalować wszystkie elementy w ramach jednej operacji.
- **Zarządzanie pakietami:** Novell Identity Manager 4.0 Advanced Edition wprowadza nowe pojęcie zwane zarządzaniem pakietami – system upraszczający tworzenie, dystrybucję i wykorzystanie wysokiej jakości elementów stanowiących treść modułowych polityk Identity Managera.
- **Sterowniki dla środowisk typu cloud:** Identity Manager 4.0 Advanced Edition wyposażony jest w szereg sterowników, umożliwiających błyskawiczną integrację z SaaS. Sterowniki zapewniają bezproblemową integrację z SaaS i rozwiązaniami rezydującymi na serwerze, udostępniając takie funkcje, jak przyznawanie i odbieranie praw dostępu, obsługa procesów wnioskowania i akceptacji, zmian haseł, aktualizacji profili oraz raportowania. Nowe sterowniki SharePoint i Salesforce.com ułatwiają integrację tożsamości korporacyjnych z aplikacjami typu cloud.
- **Wbudowane repozytorium tożsamości:** Nowa architektura Novell Identity Manager 4.0 Advanced Edition obejmuje opcjonalne, wbudowane repozytorium tożsamości (Identity Vault), dzięki czemu nie ma konieczności tworzenia i zarządzania oddzielną strukturą katalogową dla potrzeb tożsamości. Oprócz tego rodzina produktów Novell Identity Manager zawiera sterowniki zapewniające łatwą integrację wbudowanego repozytorium Identity Vault z innymi istniejącymi w przedsiębiorstwie repozytoriami informacji o tożsamości, takimi jak Active Directory czy rozmaite bazy danych.
- **Uproszczone zarządzanie tożsamością i rolami:** Novell Identity Manager 4.0 Advanced Edition upraszcza integrację różnorodnych repozytoriów ról w jednym miejscu, eliminując konieczność zarządzania oddzielnymi źródłami informacji o tożsamości. Wyposażony w intuicyjny interfejs administrator ds. mapowania ról może nawet mapować w systemie Identity Manager role i profile zdefiniowane w rozwiązaniach producentów niezależnych.
- **Usprawnione narzędzia:** Designer to ważne narzędzie, zawierające informacje biznesowe i techniczne pozwalające tworzyć rozwiązania Identity Manager dopasowane do konkretnych potrzeb. W wersji Designer 4.0 wprowadzono szereg ulepszeń – ich szczegółową listę można znaleźć pod adresem www.novell.com/documentation/designer40/resources/whatsnew/index.html. Oprócz tego Identity Manager wyposażony jest w narzędzie upraszczające proces analizowania i oczyszczania danych – Analityk 1.2.

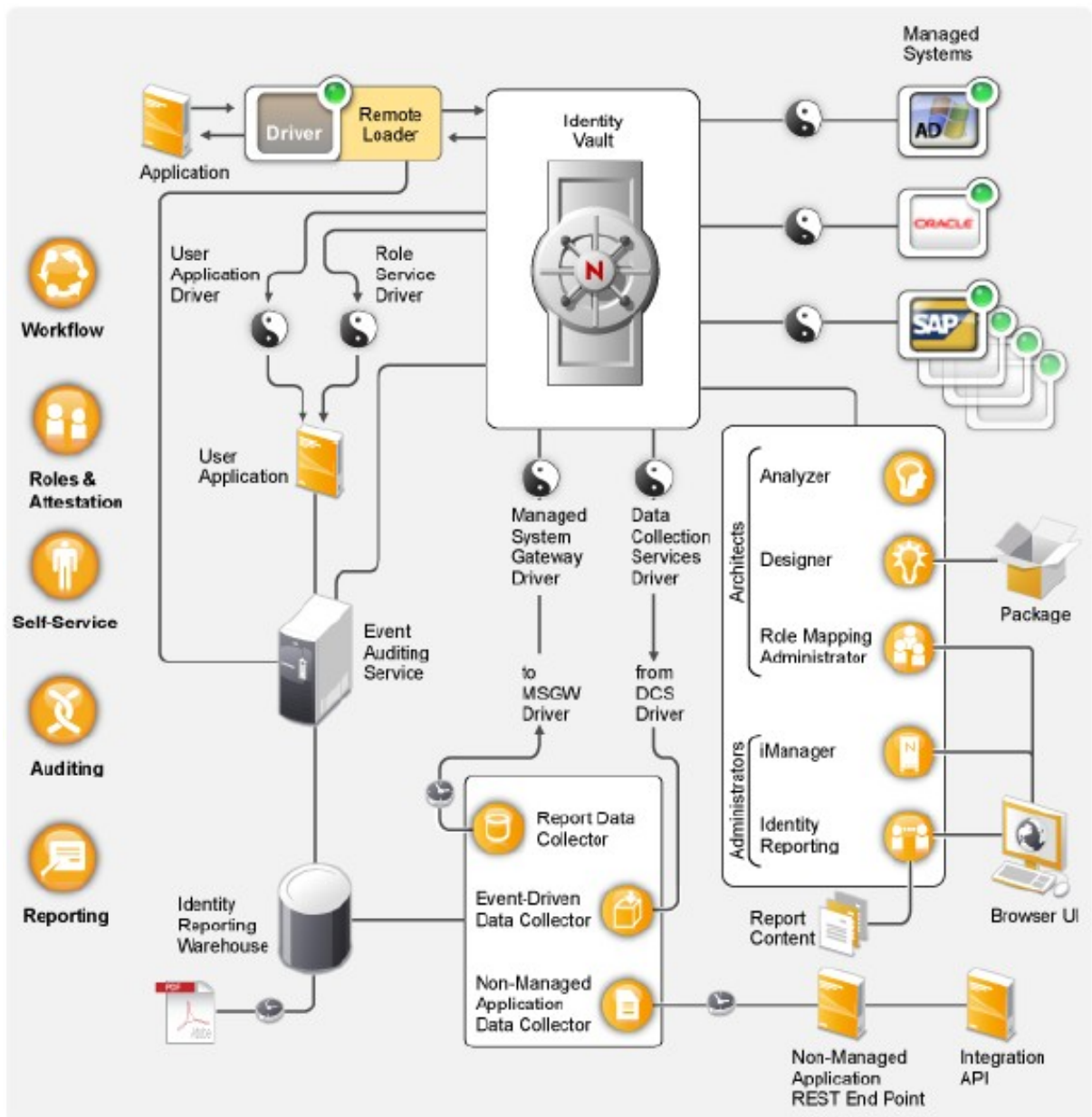
Architektura systemu

Synchronizacja danych

Synchronizacja danych jest fundamentem automatyzacji procesów biznesowych. W najprostszej formie, synchronizacja danych oznacza przesyłanie danych z miejsca, gdzie zostały one zmienione, do innych miejsc, w których są one potrzebne. Na przykład jeśli numer telefonu pracownika zostanie zmieniony w bazie systemu kadrowego firmy, zmiana ta zostanie automatycznie odzwierciedlona we wszystkich innych systemach, w których numer ten jest przechowywany.

Identity Manager nie jest ograniczony do synchronizacji danych o tożsamości. Identity Manager może synchronizować dowolny rodzaj danych przechowywanych w dołączonej aplikacji lub wbudowanym repozytorium Identity Vault.

Synchronizacja danych, łącznie z synchronizacją haseł, realizowana jest przez pięć głównych elementów rozwiązania Identity Manager: repozytorium Identity Vault, silnik Identity Managera, sterowniki (Drivers), mechanizm Remote Loader oraz dołączone aplikacje. Elementy te ukazane są w górnej części rys. 11 prezentującym architekturę wysokiego poziomu i wszystkie elementy odpowiedzialne za możliwości Novell Identity Managera.



Rys. 11 Novell Identity Manager Advanced Edition – architektura wysokiego poziomu

Elementy architektury związane z synchronizacją danych

Identity Vault: Repozytorium Identity Vault pełni rolę metakatalogu danych, które mają być synchronizowane między aplikacjami. Na przykład dane synchronizowane między systemem PeopleSoft i Lotus Notes są najpierw dodawane do repozytorium Identity Vault, a następnie wysyłane do systemu Lotus Notes. Oprócz tego Identity Vault przechowuje informacje specyficzne dla Identity Managera, takie jak konfiguracje sterowników, parametry i polityki.

Silnik Identity Managera: Gdy dane w repozytorium Identity Vault lub dołączonej aplikacji ulegają zmianie, silnik Identity Managera przetwarza wprowadzone zmiany. W przypadku zmian zachodzących w Identity Vault, silnik przetwarza zmiany i za pośrednictwem sterownika przekazuje instrukcje aplikacji. W przypadku zmian zachodzących w aplikacji, silnik odbiera informacje o zmianach od sterownika, przetwarza zmiany i przekazuje instrukcje dla repozytorium Identity Vault. Silnik Identity Managera zwany jest również silnikiem metakatalogowym.

Sterownik: Sterowniki (drivers) zapewniają połączenie z aplikacjami, których informacje o tożsamości mają podlegać zarządzaniu. Sterownik ma dwa podstawowe zadania: przekazywanie informacji o zmianach w aplikacji (zdarzeniach) do silnika Identity Managera oraz przekazywanie informacji o zmianach danych (instrukcji) od silnika Identity Managera do aplikacji.

Remote Loader: Sterowniki muszą być instalowane i uruchomione na tym samym serwerze, co aplikacja z którą zapewniają połączenie. Jeśli aplikacja znajduje się na tym samym serwerze, co silnik Identity Managera, wystarczy zainstalować sterownik na tym serwerze. Jeśli jednak aplikacja znajduje się na innym serwerze (inaczej mówiąc, jest zdalna, a nie lokalna w stosunku do silnika), na serwerze aplikacji trzeba zainstalować sterownik i Remote Loader. Remote Loader ładuje sterownik i zapewnia sterownikowi komunikację z silnikiem Identity Managera.

Aplikacja: System, katalog, baza danych lub system operacyjny, z którym łączy się sterownik. Aplikacja musi udostępniać interfejsy programistyczne (API), które pozwolą sterownikowi określać zmiany danych dokonanych przez aplikację oraz wprowadzanie zmian danych wewnątrz niej. Aplikacje nazywane są często systemami dołączonymi.

Najważniejsze pojęcia związane z synchronizacją danych

Kanały: Dane przepływają między repozytorium Identity Vault a dołączonym systemem dwoma oddzielnymi kanałami. Kanał abonencki zapewnia przepływ danych z repozytorium Identity Vault do systemu dołączonego – inaczej mówiąc, dołączony system abonuje dane z Identity Vault. Kanał publikacyjny zapewnia przepływ danych z systemów dołączonych do repozytorium Identity Vault – inaczej mówiąc, system dołączony publikuje dane dla Identity Vault.

Reprezentacja danych: Dane przekazywane są kanałami w postaci dokumentów XML. Dokument XML jest tworzony w przypadku zaistnienia zmiany w repozytorium Identity Vault lub systemie dołączonym. Dokument XML przekazywany jest do silnika Identity Managera, który przetwarza go za pomocą zestawu filtrów i polityk powiązanych z kanałem sterownika. Po przetworzeniu dokumentu XML, silnik Identity Managera wykorzystuje dokument do zainicjowania odpowiednich zmian w Identity Vault (kanał publikacyjny) lub sterownik używa dokumentu do zainicjowania odpowiednich zmian w systemie dołączonym (kanał abonencki).

Modyfikacja danych: Podczas przepływu dokumentów XML przez kanał sterownika, zawarte w dokumencie dane są modyfikowane przez polityki powiązane z kanałem. Polityki wykorzystywane są do wielu celów, w tym zmiany formatów danych, mapowania atrybutów pomiędzy repozytorium Identity Vault i systemem dołączonym, warunkowego blokowania przepływu danych, generowania powiadomień e-mail oraz modyfikowania rodzaju zmiany danych.

Kontrola przepływu danych: Przepływem danych sterują filtry lub polityki filtrów. Filtry określają, które elementy danych podlegają synchronizacji między repozytorium Identity Vault i systemem dołączonym. Na przykład synchronizacji między systemami podlegają zazwyczaj dane użytkownika, dlatego w przypadku większości dołączonych systemów są one uwzględnione w filtrze. Jednakże drukarki leżą zwykle poza obszarem zainteresowania większości aplikacji, więc w przypadku większości systemów dołączonych dane o drukarkach nie figurują w filtrach.

Każda relacja między repozytorium Identity Vault a systemem dołączonym ma dwa filtry: filtr na kanale abonenckim, sterujący przepływem danych z repozytorium Identity Vault do systemu dołączonego, oraz filtr na kanale publikacyjnym, sterujący przepływem danych z systemu dołączonego do repozytorium Identity Vault.

Źródła autorytatywne: Większość elementów danych powiązanych z tożsamością ma swojego właściciela. Właściciel elementu danych uznawany jest za jego źródło autorytatywne. Ogólnie rzecz biorąc, jedynie źródło autorytatywne danego elementu danych ma prawo dokonywać jego zmiany.

Na przykład za autorytatywne źródło adresu e-mail pracownika uznawany jest korporacyjny system poczty elektronicznej. Jeśli administrator korporacyjnego katalogu (*white pages*) zmienia w tym systemie adres e-mail pracownika, zmiana ta nie ma wpływu na to, czy pracownik otrzyma pocztę kierowaną na ten adres, ponieważ aby zmiana odniosła skutek, musi być wprowadzona w systemie poczty elektronicznej.

Do określania autorytatywnych źródeł dla poszczególnych elementów Identity Manager używa filtrów. Na przykład jeśli filtr dla relacji między wewnętrzną centralą telefoniczną a Identity Vault dopuszcza przepływ numeru telefonu pracownika z systemu centrali do Identity Vault, ale nie z Identity Vault do systemu centrali, system centrali jest autorytatywnym źródłem numeru telefonu. Jeśli relacje z wszelkimi innymi systemami dołączonymi dopuszczają przepływ numeru telefonu z Identity Vault do systemu dołączonego, ale nie odwrotnie, w efekcie ostatecznym system wewnętrznej centrali telefonicznej będzie jedynym autorytatywnym źródłem numeru telefonu w przedsiębiorstwie.

Zautomatyzowane konfigurowanie kont użytkowników: Zautomatyzowane konfigurowanie kont użytkowników oznacza zdolność Identity Managera do wykonywania działań związanych z konfigurowaniem kont użytkowników wykraczających poza prostą synchronizację danych.

Na przykład w typowym systemie Identity Manager, w którym baza danych systemu kadrowego jest autorytatywnym źródłem większości danych o pracowniku, dodanie pracownika do bazy systemu kadrowego powoduje automatyczne utworzenie odpowiedniego konta w repozytorium Identity Vault. Z kolei utworzenie konta w repozytorium Identity Vault powoduje automatyczne utworzenie w systemie poczty elektronicznej konta e-mail pracownika. Dane konieczne do skonfigurowania konta e-mail pracownika pobierane są z repozytorium Identity Vault i mogą obejmować nazwisko, miejsce pracy, numer telefonu itd.

Zautomatyzowanym konfigurowaniem kont, praw dostępu i danych można kierować na szereg różnych sposobów, w tym poprzez:

- **Wartości elementów danych:** Na przykład automatyczne tworzenie konta w bazach danych dostępu do budynków firmy może być uzależnione od wartości atrybutu lokalizacji użytkownika
- **Schematy przekazywania zadań akceptacji:** Na przykład dodanie pracownika do działu finansowego może spowodować automatyczne wysłanie listu do szefa działu finansowego z wnioskiem o akceptację utworzenia konta nowego pracownika w systemie finansowym. Szef działu finansowego kierowany jest przez e-mail do strony, na której akceptuje lub odrzuca wniosek. Akceptacja powoduje automatyczne utworzenie konta pracownika w systemie finansowym.
- **Przypisanie ról:** Przykładowo, pracownik otrzymuje rolę księgowego. Identity Manager przydziela mu wszelkie konta, prawa dostępu i dane przypisane do roli księgowego, albo z użyciem schematów systemowych (bez udziału człowieka), z uwzględnieniem schematów przekazywania zadań lub z użyciem kombinacji obu wariantów.

Upoważnienia: Upoważnienie oznacza zasób systemu dołączonego, taki jak konto lub członkostwo w grupie. Gdy użytkownik spełnia kryteria ustanowione dla upoważnienia w systemie dołączonym, Identity Manager przetwarza zdarzenie, czego efektem jest przyznanie użytkownikowi dostępu do zasobu, oczywiście pod warunkiem zgodności z szeregiem polityk. Na przykład jeśli użytkownik spełnia kryteria wymagane dla konta Exchange w Active Directory, Identity Manager przetwarza zdarzenie z uwzględnieniem zestawu polityk Active Directory sterownika dla konta Exchange.

Największą zaletą upoważnień jest możliwość zdefiniowania logiki biznesowej dla dostępu do zasobów w jednym upoważnieniu, zamiast w wielu politykach sterowników. Przykładowo można zdefiniować

upoważnienie konta, dające użytkownikowi konta w czterech systemach dołączonych. Decyzja o przydzieleniu użytkownikowi konta określona jest w upoważnieniu, co oznacza, że polityki dla każdego z czterech sterowników nie muszą zawierać logiki biznesowej, a jedynie określać mechanizm przydzielania konta. Jeśli trzeba dokonać zmiany logiki biznesowej, wystarczy zmienić ją w upoważnieniu, zamiast w czterech sterownikach.

Zadania: W większości przypadków Identity Manager działa w odpowiedzi na zmiany danych lub wnioski użytkowników. Przykładowo, gdy jakieś dane zmieniają się w jednym systemie, Identity Manager dokonuje odpowiednich zmian w innych systemach lub jeśli użytkownik wnioskuje o dostęp do systemu, Identity Manager inicjuje odpowiednie procesy (przekazywanie zadań, udostępnianie zasobów itd.), aby zapewnić ten dostęp.

Zadania umożliwiają Identity Managerowi wykonywanie działań nie zainicjowanych zmianami danych lub wnioskami użytkowników. Zadanie składa się z danych konfiguracyjnych, przechowywanych w repozytorium Identity Vault, oraz odpowiedniego kodu realizacyjnego. Identity Manager zawiera wstępnie zdefiniowane zadania dla takich działań, jak uruchamianie i zatrzymywanie sterowników, wysyłanie pocztą elektroniczną powiadomień o wygasaniu ważności haseł czy sprawdzanie stanu sterowników. Można także tworzyć własne zadania realizujące inne działania; wymaga to oczywiście napisania odpowiedniego kodu przez administratora, programistę lub konsultanta.

Zlecenia: Zmiany danych w repozytorium Identity Vault lub systemach dołączonych są zwykle przetwarzane niezwłocznie. Zlecenia pozwalają zaplanować działania, które mają być wykonane określonego dnia o określonej godzinie. Na przykład nowo zatrudniony pracownik ma rozpocząć pracę w następnym miesiącu. Należy go już dodać do bazy danych systemu kadrowego, jednak nie powinien uzyskać dostępu do poczty elektronicznej i innych zasobów korporacyjnych przed rozpoczęciem pracy. Zlecenie pozwala udostępnić mu odpowiednie zasoby w dokładnie określonym momencie.

Przekazywanie zadań, role, poświadczenia i samoobsługa

Identity Manager zawiera wyspecjalizowany moduł – aplikację użytkownika (User application), który obsługuje przekazywanie danych, przypisywanie ról, poświadczenia oraz samoobsługę w zakresie tożsamości.

Standardowa wersja aplikacji użytkownika wchodzi w skład Identity Managera. Standardowa wersja zapewnia użytkownikom mechanizmy samoobsługi, ułatwiające przypomnienie lub zresetowanie zapomnianych haseł, diagramy organizacyjne do zarządzania informacjami użytkowników w firmowym katalogu, funkcje zarządzania użytkownikami pozwalające na tworzenie kont użytkowników w repozytorium Identity Vault, a także podstawowe samoobsługowe funkcje tożsamości, takie jak zarządzanie informacjami w profilu użytkownika.

Zawarty w aplikacji użytkownika moduł definiowania kont w oparciu o role stanowi część Novell Identity Manager 4.0 Advanced Edition. Dołączona jest również standardowa aplikacja użytkownika z zaawansowanymi mechanizmami samoobsługi, przekazywania zadań związanych z akceptacją wniosków, udostępniania zasobów w oparciu o role, ograniczeń rozdzielania obowiązków oraz poświadczeń. Novell Identity Manager 4.0 Advanced Edition dysponuje zarówno możliwościami wersji standardowej, jak i modułu definiowania kont w oparciu o role.

Elementy architektury związane z przekazywaniem zadań, rolami, poświadczeniami i samoobsługą

Aplikacja użytkownika: Aplikacja użytkownika to obsługiwana za pomocą przeglądarki aplikacja internetowa, umożliwiająca użytkownikom i administratorom biznesowym wykonywanie szeregu czynności

samoobsługowych związanych z tożsamością i udostępnianiem zasobów w oparciu o role, w tym zarządzanie hasłami i danymi tożsamości, inicjowanie i monitorowanie realizacji wniosków o przyznanie dostępu i przypisanie ról, zarządzanie procesem akceptacji wniosków o przyznanie dostępu oraz weryfikowanie raportów poświadczania. Aplikacja zawiera silnik przekazywania zadań, sterujący przekazywaniem wniosków zgodnie z odpowiednim procesem akceptacji.

Sterownik aplikacji użytkownika: Sterownik aplikacji użytkownika przechowuje informacje konfiguracyjne i powiadamia aplikację o wystąpieniu zmian w repozytorium Identity Vault. Można go również skonfigurować tak, by zdarzenia w repozytorium Identity Vault uruchamiały procesy przekazywania zadań i by informacje o pozytywnym bądź negatywnym zakończeniu tych procesów trafiały do aplikacji użytkownika i były przekazywane wnioskującym.

Sterownik usług dla ról i zasobów: Sterownik usług dla ról i zasobów zarządza wszystkimi przypisaniami ról i zasobów, uruchamiały procesy przekazywania zadań dla wniosków o akceptację przypisania ról i zasobów, a także realizuje pośrednie przypisania ról wynikające z przynależności użytkownika do grup. Sterownik również przyznaje i odbiera upoważnienia w oparciu o role przypisane użytkownikom i wykonuje czynności porządkowe po zakończeniu obsługi wniosków.

Najważniejsze pojęcia związane z przekazywaniem zadań, rolami, poświadczeniami i samoobsługą

Udostępnianie zasobów w oparciu o przekazywanie zadań: Udostępnianie zasobów w oparciu o przekazywanie zadań umożliwia użytkownikom składanie wniosków o przyznanie dostępu do zasobów. Wniosek taki przekazywany jest zgodnie ze zdefiniowanym wcześniej schematem, który może uwzględniać konieczność akceptacji przez jedną lub więcej osób. Jeśli akceptacje zostaną przyznane, użytkownik uzyskuje dostęp do zasobów. Wnioski o przyznanie dostępu do zasobów mogą być również generowane pośrednio w odpowiedzi na zdarzenia zachodzące w repozytorium Identity Vault. Przykładowo, dodanie użytkownika do grupy może zainicjować wniosek o przyznanie mu dostępu do określonych zasobów.

Udostępnianie zasobów w oparciu o role: Udostępnianie zasobów w oparciu o role umożliwia użytkownikom uzyskanie dostępu do określonych zasobów w oparciu o przypisane im role. Użytkownik może mieć przypisaną jedną lub więcej ról. Jeśli przypisanie roli wymaga akceptacji, wniosek o przypisanie roli inicjuje proces przekazywania zadań związanych z jego akceptacją.

Rozdzielenie obowiązków: Aby zapobiec przypisaniu użytkownikom konfliktowych ról, zawarty w aplikacji użytkownika moduł definiowania kont w oparciu o role wyposażony jest w funkcję rozdzielania obowiązków. Można ustanowić ograniczenia definiujące, które role uważane są za konfliktowe.

W przypadku pojawienia się konfliktu ról, mechanizm rozdzielania obowiązków pozwala zaakceptować lub odrzucić wyjątek od ograniczeń. Zaakceptowane wyjątki są rejestrowane jako naruszenia rozdzielania obowiązków i mogą podlegać weryfikacji w opisanym poniżej procesie poświadczania.

Zarządzanie rolami: Zarządzanie rolami musi być prowadzone przez osoby pełniące rolę administratora modułu ról lub menedżera ról. Administrator modułu ról tworzy nowe role oraz modyfikuje i usuwa istniejące role, modyfikuje relacje między rolami, przyznaje i odbiera przypisania ról użytkownikom, a także tworzy, modyfikuje i usuwa ograniczenia rozdzielania obowiązków.

Menedżer ról ma te same uprawnienia, co administrator modułu ról, z wyjątkiem zarządzania ograniczeniami rozdzielania obowiązków, konfigurowania systemu ról oraz uruchamiania raportów. Administrator modułu ról ma nieograniczony dostęp do systemu ról, zaś zakres działań menedżera ról ograniczony jest do określonych użytkowników, grup i ról.

Poświadczenie: Przypisanie ról określa dostęp użytkownika do zasobów firmy, zaś nieprawidłowe przypisanie może zagrażać zgodności z wewnętrznymi regulacjami i przepisami prawa. Identity Manager pomaga w weryfikacji prawidłowości przypisania ról za pomocą procesu poświadczenia. Korzystając z tego procesu, użytkownicy mogą weryfikować informacje zawarte we własnym profilu, zaś menedżerowie ról mogą weryfikować przypisanie ról oraz naruszenia rozdzielania obowiązków.

Audytywanie i raportowanie

Audytywanie i raportowanie realizowane jest przez będący nowością w systemie Novell Identity Manager 4.0 Advanced Edition moduł raportowania tożsamości. Generuje on raporty dostarczające newralgicznych informacji biznesowych dotyczących różnych aspektów danej konfiguracji Identity Managera, w tym informacji pochodzących z repozytoriów Identity Vault i zarządzanych systemów, takich jak Active Directory lub SAP. Moduł raportowania tożsamości wykorzystuje następujące elementy:

Usługa audytu zdarzeń: Usługa gromadząca zapisywane w rejestrach zdarzenia związane z działaniami wykonywanymi w module raportowania, takimi jak import, modyfikacja, usuwanie lub planowanie raportu. Usługa audytu zdarzeń (Event Auditing Service, EAS) gromadząca zapisywane w rejestrach zdarzenia związane z działaniami wykonywanymi w module udostępniania zasobów w oparciu o role (Roles Based Provisioning Module, RBPM) i administratora mapowania ról (Role Mapping Administrator, RMA).

Hurtownia informacji o tożsamości: Repozytorium następujących informacji:

- Informacje o zarządzaniu raportami (takie jak definicje raportów, harmonogramy raportów i wykonane raporty), widoki baz danych wykorzystywane do raportowania oraz informacje o konfiguracji.
- Dane o tożsamości zebrane przez Report Data Collector, Event-Driven Data Collector i Non-Managed Application Data Collector.
- Dane audytorskie, obejmujące zdarzenia zebrane przez usługę audytu zdarzeń.

Hurtownia informacji o tożsamości przechowuje swoje dane w bazie danych SIEM (*Security Information & Event Management*).

Usługa zbierania danych: Usługa gromadząca informacje z różnych źródeł w firmie. Usługa zbierania danych obejmuje trzy usługi składowe:

- **Report Data Collector:** Korzystając z modelu *pull* zbiera dane z jednego lub więcej repozytoriów Identity Vault. Zbieranie ma charakter periodyczny, zgodnie z zestawem parametrów konfiguracyjnych. Do zbierania danych wykorzystuje sterownik Managed System Gateway.
- **Event-Driven Data Collector:** Korzystając z modelu *push*, gromadzi dane o zdarzeniach zbierane przez sterownik Data Collection Service.
- **Non-Managed Application Data Collector:** Pobiera dane z jednej lub większej liczby niezarządzanych aplikacji za pomocą punktu końcowego REST, napisanego specjalnie dla każdej aplikacji. Aplikacje niezarządzane w obrębie firmy to te, które nie są dołączone do repozytorium Identity Vault.

Sterownik usługi zbierania danych: Sterownik zbierający informacje o zmianach obiektów składowanych w repozytorium Identity Vault, takich jak konta, role, zasoby, grupy i przynależność do zespołów. Sterownik usługi zbierania danych rejestruje się w usłudze zbierania danych i przekazuje do niej zdarzenia zmiany danych (takie jak synchronizacja danych, dodawanie, modyfikacja i usuwanie).

Zebrane informacje rejestrują zmiany następujących obiektów:

- Konta użytkowników i tożsamości
- Role i poziomy ról
- Grupy

UWAGA: Moduł raportowania nie obsługuje grup dynamicznych, generuje jedynie raporty o grupach statycznych:

- Przynależność do grup
- Definicje wniosków o przyznanie uprawnień
- Definicje i naruszenia rozdzielania obowiązków
- Powiązania upoważnień użytkowników
- Definicje i parametry zasobów
- Przypisania ról i zasobów
- Upoważnienia Identity Vault, typy upoważnień i sterowniki

Sterownik Managed System Gateway: Sterownik zbierający informacje z systemów zarządzanych. W celu zbierania danych wysyła zapytania do repozytorium Identity Vault. Zbierane dane obejmują następujące informacje:

- Listę wszystkich systemów zarządzanych
- Listę wszystkich kont w systemach zarządzanych
- Typy, wartości i przypisania upoważnień, a także profile kont użytkowników dla raportowania o tożsamości w systemach zarządzanych. Interfejs użytkownika modułu raportowania pozwala łatwo zaplanować tworzenie raportów poza godzinami szczytowego obciążenia dla optymalizacji wydajności.

Raporty: Identity Manager zawiera wstępnie zdefiniowane raporty w dogodny sposób prezentujące informacje w hurtowni informacji o tożsamości. Można także tworzyć własne raporty.

Punkt końcowy REST aplikacji niezarządzanych: Aplikacja niezarządzana to aplikacja, która nie jest dołączona do repozytorium Identity Vault, zawiera jednak dane, które powinny się znaleźć w raporcie. Zdefiniowanie punktu końcowego REST pozwala modułowi raportowania zbierać dane z tej aplikacji.

Interfejs programistyczny integracji: Pierwsze wydanie modułu raportowania o tożsamości obsługuje jeden interfejs API REST. Pozwala on zaimplementować punkt końcowy REST dla aplikacji niezarządzanych.

Narzędzia w systemie Identity Manager 4.0 Advanced Edition

Novell Identity Manager 4.0 Advanced Edition zawiera narzędzia pozwalające utworzyć rozwiązanie Identity Manager i zarządzać nim. Każde z nich ma określone przeznaczenie.

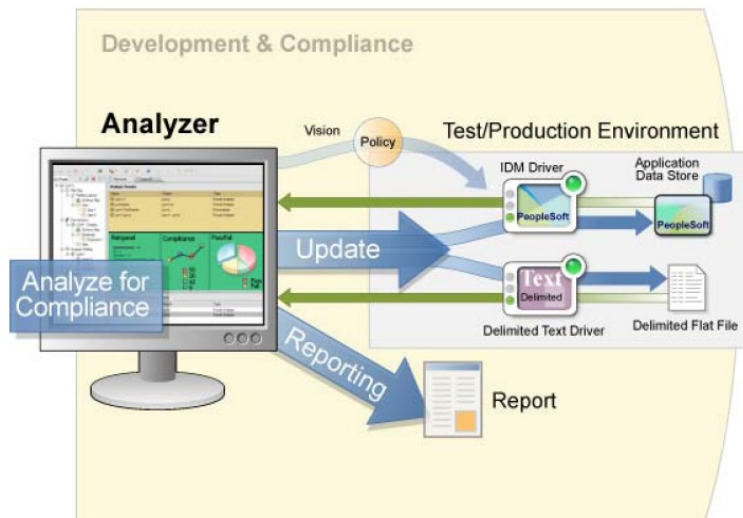
Narzędzie Designer służy do projektowania, tworzenia i konfigurowania systemu Identity Manager w środowisku off-line, a następnie wdrażania zmian w środowisku produkcyjnym. Designer udostępnia również mechanizmy zarządzania pakietami dla wstępnego konfigurowania i dostosowywania polityk sterowników Identity Managera. Analityk pozwala analizować, oczyszczać i przygotowywać dane do synchronizacji podczas tworzenia rozwiązania Identity Manager.

Role Mapping Administrator – administrator ds. mapowania ról – służy do tworzenia i zarządzania rolami w rozwiązaniu Identity Manager.

Narzędzie iManager można użyć do podobnych zadań jak Designera, a także do monitorowania stanu systemu, jednak iManager nie obsługuje zarządzania pakietami. Zaleca się wykorzystanie iManagera do zadań administracyjnych, zaś Designera do konfiguracji, gdzie wymagane są zmiany pakietów, modelowanie oraz testowanie przed wdrożeniem.

Analyzer

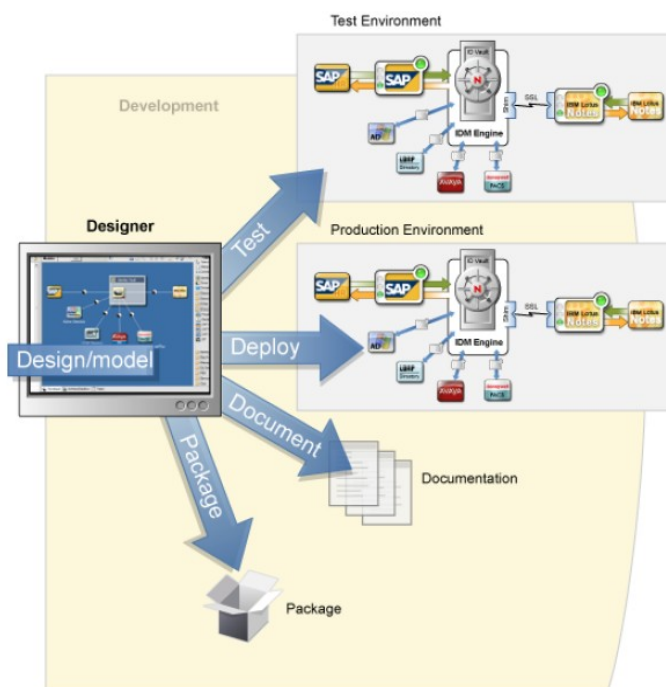
Analyzer to oparty na Eclipse zestaw narzędzi do zarządzania tożsamościami, pozwalający zapewnić egzekwowanie wewnętrznych polityk jakości danych za pomocą analizy, oczyszczania, uzgadniania i monitorowania danych oraz raportowania. Analyzer umożliwia analizowanie, optymalizację i kontrolowanie wszystkich składnic danych w przedsiębiorstwie.



Rys. 12 Identity Manager – Analyzer

Designer

Designer to oparte na Eclipse narzędzie do projektowania, wdrażania i dokumentowania systemu Identity Manager. Korzystając z graficznego interfejsu użytkownika Designera, można projektować i testować system w środowisku offline, wdrażać go w środowisku produkcyjnym i dokumentować wszelkie szczegóły wdrożonego systemu.



Rys. 13 Identity Manager – Designer

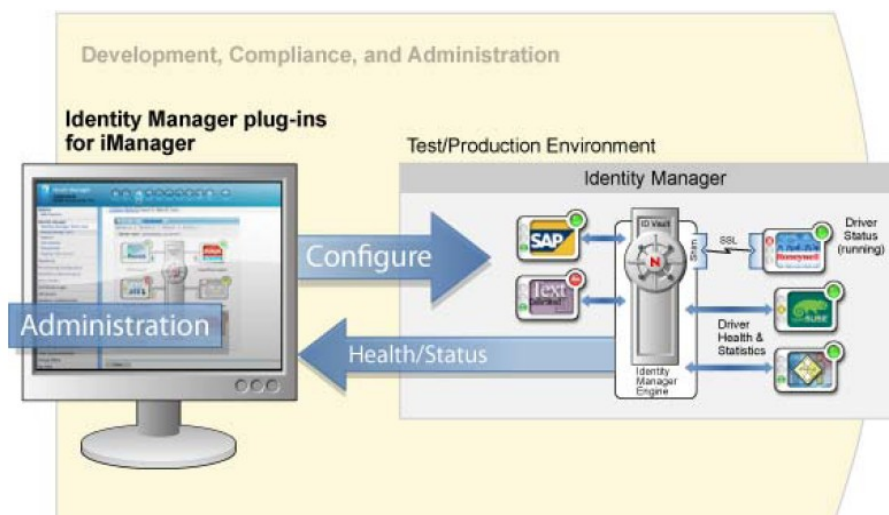
Projektowanie: Designer udostępnia graficzny interfejs umożliwiający modelowanie systemu. Obejmuje on widoki pozwalające tworzyć i kontrolować połączenia między Identity Managerem i aplikacjami, konfigurować polityki i modelować przepływ danych między dołączonymi aplikacjami.

Wdrażanie: Projekt wykonany za pomocą Designera wdraża się w środowisku produkcyjnym dopiero po zainicjowaniu wdrożenia. Daje to swobodę eksperymentowania, testowania wyników i rozwiązywania wszelkich problemów przed rozpoczęciem eksploatacji w środowisku produkcyjnym.

Dokumentowanie: Narzędzie pozwala tworzyć obszerną dokumentację ukazującą hierarchię systemów, konfiguracje sterowników i polityk itd. Dokumentacja może zawierać wszelkie informacje konieczne do zrozumienia technicznych aspektów systemu, jest też pomocna przy weryfikacji zgodności z wymogami wewnętrznymi polityk i przepisów prawa.

iManager

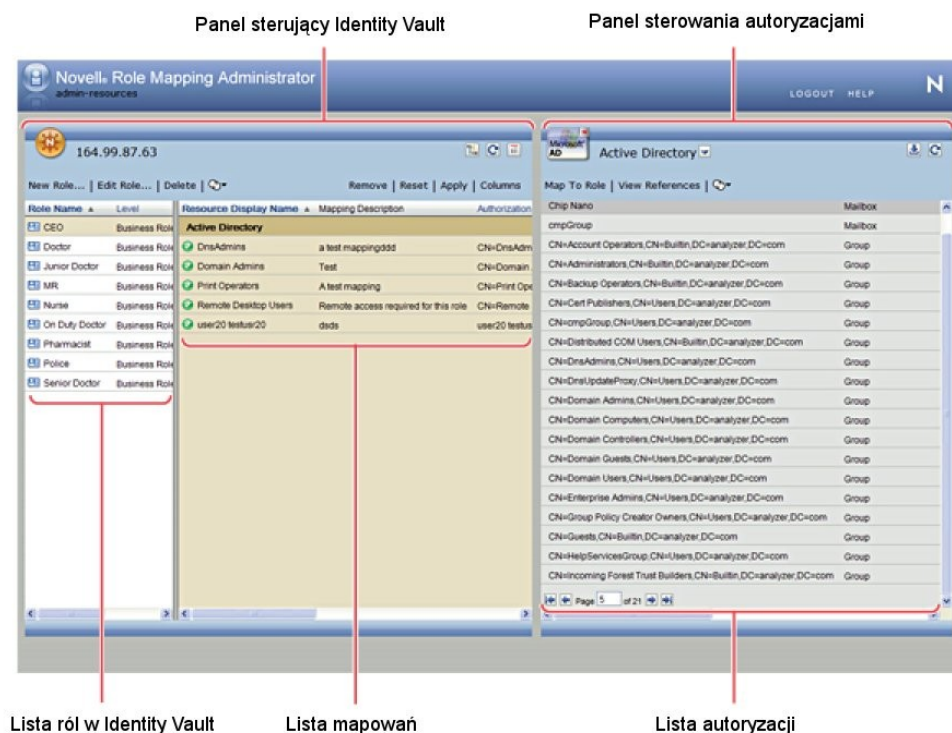
Novell iManager to wykorzystujące przeglądarkę internetową narzędzie udostępniające pojedynczy punkt administrowania wieloma produktami Novella, w tym również Identity Managerem. Korzystając z odpowiednich wtyczek, za pomocą iManagera można zarządzać systemem Identity Manager i uzyskiwać aktualne informacje o jego stanie.



Rys. 14 Novell iManager

Administrator mapowania ról

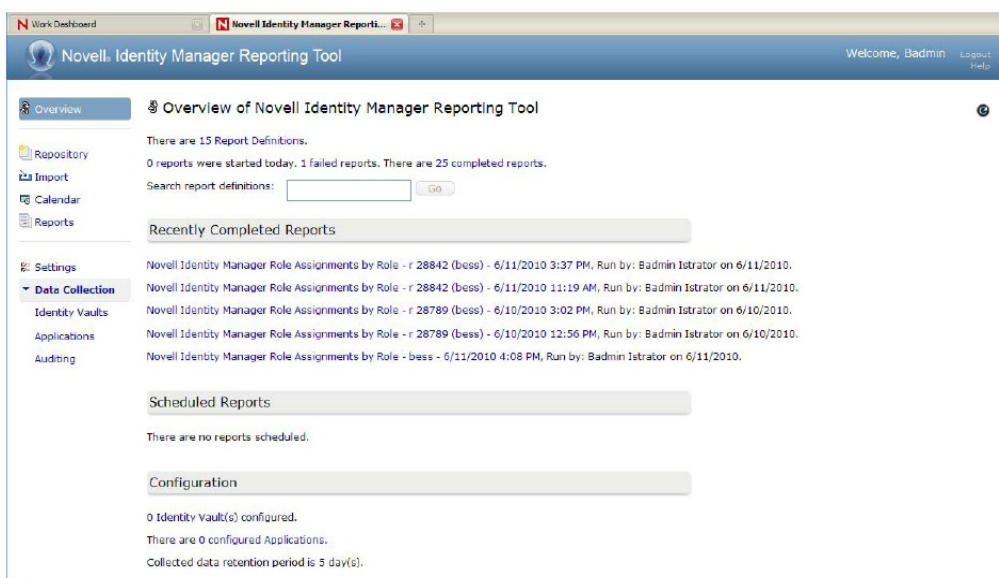
Administrator mapowania ról (Role Mapping Administrator) to usługa sieciowa umożliwiająca wykrywanie autoryzacji i zezwoleń przyznawanych w dużych systemach informatycznych. Umożliwia to analitykom biznesowym, nie tylko administratorom, definiowanie i egzekwowanie przypisania autoryzacji do ról biznesowych.



Rys. 15 Role Mapping Administrator

Raportowanie o tożsamości

Moduł raportowania o tożsamości generuje raporty ukazujące newralgiczne informacje biznesowe, dotyczące różnych aspektów konfiguracji systemu Novell Identity Manager 4.0 Advanced Edition, w tym informacji zebranych z repozytoriów Identity Vault i systemów zarządzanych takich jak Active Directory lub SAP. Moduł raportowania udostępnia zestaw wstępnie zdefiniowanych, gotowych do użycia raportów. Umożliwia także importowanie dowolnych raportów zdefiniowanych za pomocą narzędzi innych producentów. Interfejs użytkownika modułu raportowania pozwala łatwo planować wykonywanie raportów poza godzinami szczytowego obciążenia w celu optymalizacji wydajności systemów.



Rys. 16 Moduł raportowania o tożsamości

Moduł raportowania zapewnia duże możliwości integracji. Przykładowo, jeśli zamierza się zbierać dane na temat pochodzących od niezależnych dostawców aplikacji, które nie są połączone z Identity Managerem, można zaimplementować własny punkt końcowy REST, pozwalający zbierać dane z tych aplikacji. Można także dostosować dane wysyłane do repozytorium Identity Vault. Gdy dane będą dostępne, można utworzyć własne raporty ukazujące te informacje.

Podsumowanie

Przedsiębiorstwa nieustannie zmagają się z czasochłonnymi, ręcznymi procesami konfigurowania dostępu do zasobów w ramach wszystkich systemów, aplikacji i urządzeń w firmie i związanymi z tym szybko rosnącymi kosztami. Rozwiązanie Novell Identity Manager upraszcza zarządzanie tożsamością już na etapie przyjmowania nowych pracowników do firmy, wprowadzania zmian w strukturze zatrudnienia bądź redukcji liczby personelu, nawiązywania nowych relacji partnerskich czy przeprowadzania fuzji. Oprogramowanie firmy Novell automatyzuje konfigurowanie kont użytkowników i zarządzanie hasłami w całym cyklu ich eksploatacji. Zapewnia ono synchronizowanie wielu haseł z pojedynczą nazwą logowania oraz natychmiastowy dostęp do zasobów, umożliwia modyfikowanie lub odbieranie uprawnień zgodnie z potrzebami biznesowymi firmy i w ramach wszystkich posiadanych systemów. Dzięki rozwiązaniu Novell Identity Manager można kontrolować koszty administrowania użytkownikami, eliminować złożone, ręczne procesy, a także zapewnić bezpieczeństwo i egzekwować zgodność z przepisami w skali całego przedsiębiorstwa. Jednocześnie użytkownicy mogą korzystać w sposób kontrolowany z zasobów potrzebnych im do wykonywania swoich zadań.

Novell Identity Manager to najbardziej wszechstronne i skalowalne rozwiązanie do zarządzania tożsamością. Znakomicie sprawdziło się w największych przedsiębiorstwach w Polsce i na świecie, m.in. Allianz Suisse, Bank Zachodni WBK, Lufthansa, Polskie Linie Lotnicze LOT SA i TRW. Identity Manager pozwala zwiększyć zwrot z inwestycji i nawiązać bliskie relacje z klientami, partnerami oraz pracownikami dzięki usprawnieniu mechanizmów dostępu do zasobów przedsiębiorstwa.

Więcej informacji znajduje się na stronie: <http://www.novell.com/products/identitymanager/>

W celu uzyskania szczegółowych informacji o cenach i licencjonowaniu prosimy o kontakt:

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

10/10 | © 2010 Novell, Inc. Wszelkie prawa zastrzeżone. Novell, logo Novell, logo N, Novell Identity Manager, są zastrzeżonymi znakami towarowymi firmy Novell, Inc. w USA i innych krajach. * Pozostałe znaki towarowe są własnością odpowiednich podmiotów.