

Эффективное управление доступом к сетевым ресурсам

Максим Рева

mmreva@osi.in.ua

Екатерина Кружалина

katreen@osi.in.ua

26 Октябрь, 2009



Системный
интегратор

Novell®

“Исследования показывают, что компании настолько заняты отражением внешних угроз безопасности, что когда дело доходит до внутренней утечки информации, они не могут решить эту более широкую проблему...”

Потеря более **20%** конфиденциальной информации приводит к банкротству компании

60% ИТ-специалистов считают одной из ключевых угроз сотрудников компании (год назад 44%)

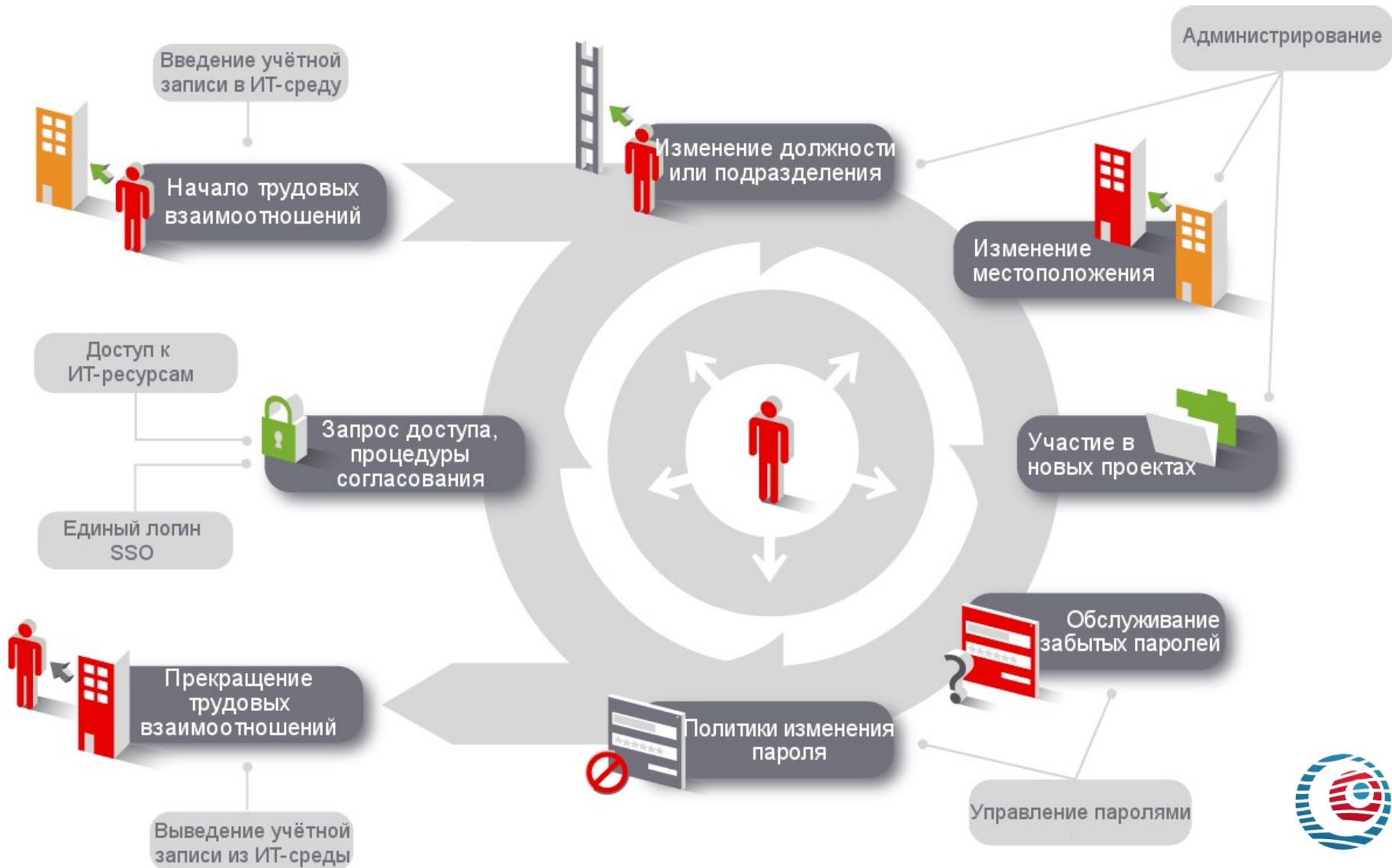
63% нарушений безопасности - человеческие ошибки

*Источники: Computing Technology Industry Assn., 2003.
ИТ исследования в Великобритании.2006-7.*

Исследования Cisco



Автоматизация управления жизненным циклом учётных записей

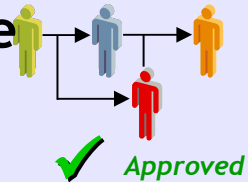


Задачи, решаемые Novell Identity Manager^N

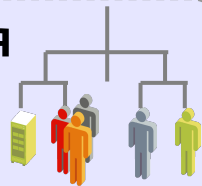
Ролевое
предоставление
доступа



Согласование
доступа к
ресурсам



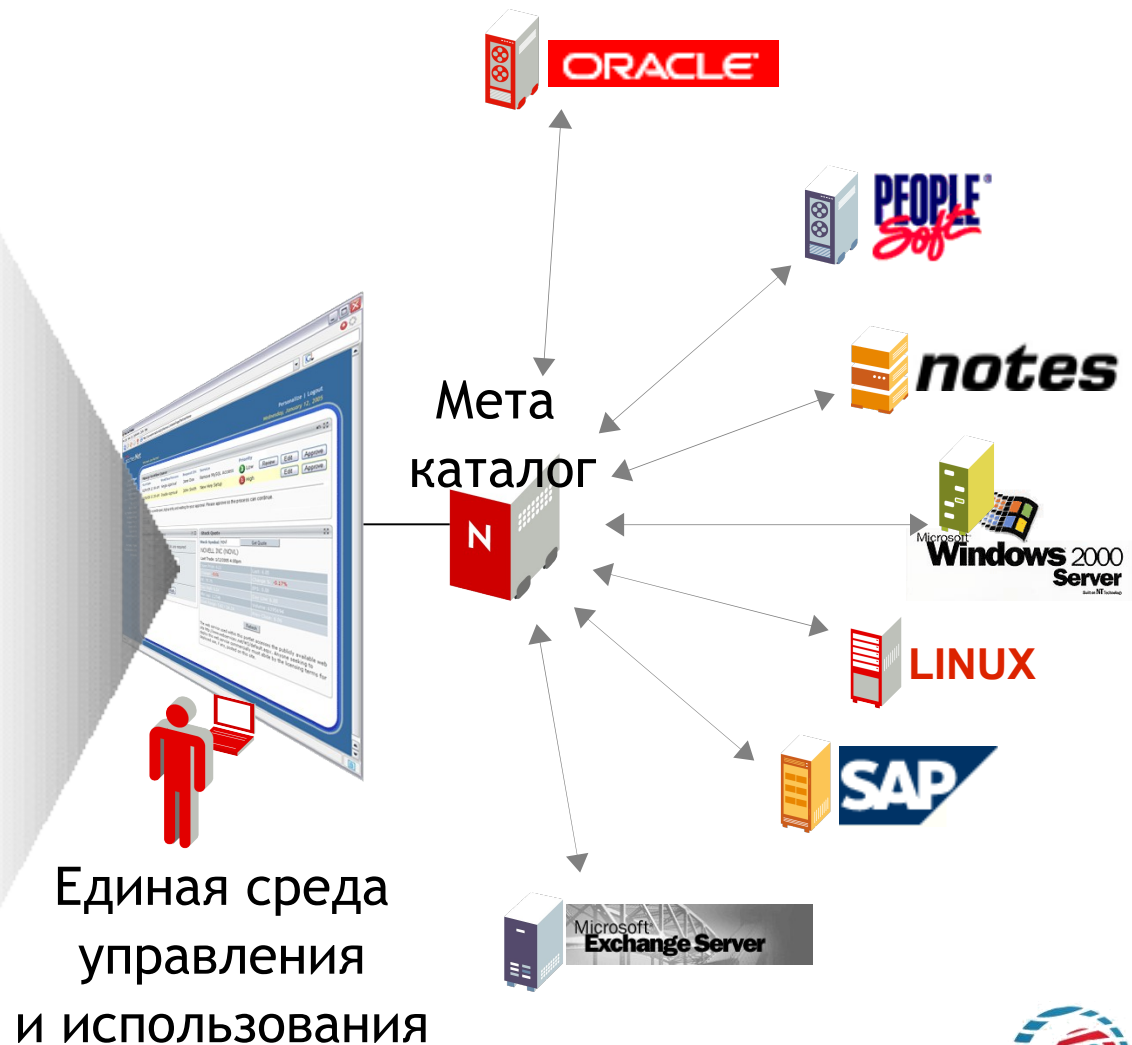
Синхронизация
учётной
информации



Управление
паролями



Корпоративный
справочник



Распределение доступов к ИТ-ресурсам на ролевой основе

Почему необходимо использовать Ролевое управление?

Уменьшение стоимости управления учётными записями:



- Владелец ресурса участвует в разграничении прав доступа, ассоциируя пользователя с небольшим количеством ролей, связанных с наборами ресурсов
- Автоматизация создания учётных записей, устраняющая ручное дублирование данных

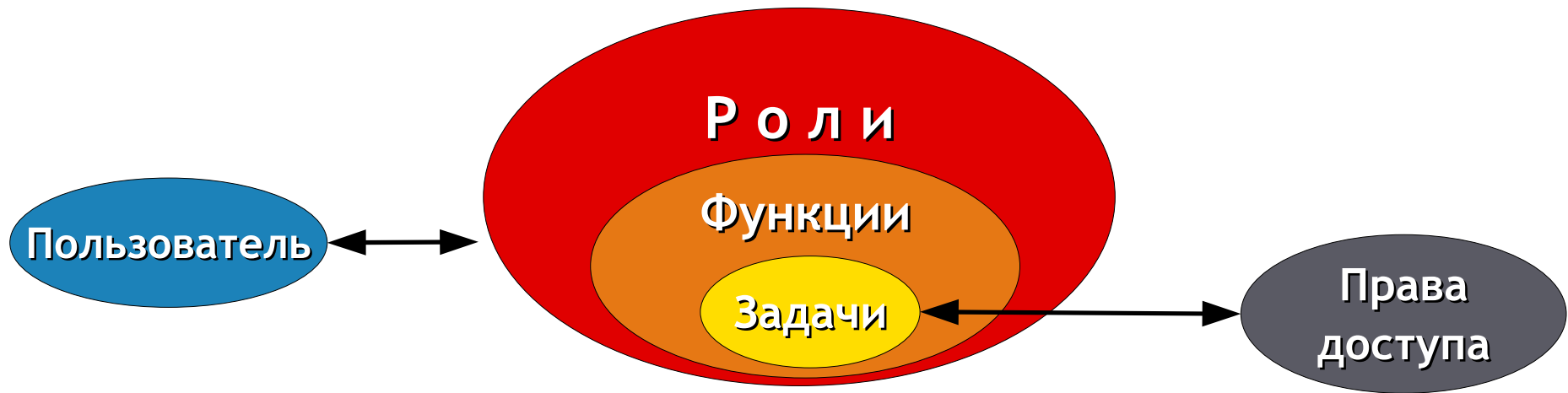
Повышение безопасности:



- Реализация принятых политик безопасности
- Динамическое изменение прав доступа при изменении статуса или роли сотрудника в организации
- Мгновенная ликвидация прав доступа
- Кардинальное уменьшение влияния человеческого фактора на процесс управления доступами



Элементы ролевого управления доступом. Role-Based Access Control



- **Пользователи** ассоциируются с одной или несколькими ролями
- Роль связана с **правами доступа**
- Права предоставляют пользователям доступ к ресурсам, требуемым для выполнения бизнес-**функций** и **задач**
- **Роль** — набор бизнес-функций, задач и необходимых прав доступа к ресурсам



Доступы на основе ролей

- Рольевое назначение может иметь временное ограничение
- Описание конфликтных ролей
- Отслеживание конфликтных ситуаций
 - пользователь имеет возможность запросить доступ, предоставляемый через конфликтную роль
 - проведение ассоциации по конфликтным ролям после подтверждения владельца ресурса и процедуры согласования
 - > всегда аудирруется
 - > всегда в отчётах выделяется как конфликтное назначение доступа
 - конфликтное назначение всегда требует временного ограничения



Оперативная отчётность

- Кто ассоциирован с конкретной ролью?
- Какими доступами (ролями) пользуется пользователь?
- Какие у роли подчинённые роли?
- Есть ли у роли конфликтные роли?
- Текущее состояние конфликтов по ролям?
- У кого в ближайшее время заканчивается период использования доступа, предоставляемого ролью?
- Какой ролевой доступ запрошен конкретным пользователем?



Аттестация

Novell iManager

Role Assignment Attestation

Request Role Assignment Attestation Process

Submit a request for a new Role Assignment Attestation, re-launch an existing one, or save request details. (* - indicates required.)

Use a Saved Request

Selected Process Request: Default

Enter a label and description for the attestation request. The Display Label appears in the My Tasks list, the list of saved requests, and other display lists as the name of the attestation request. The Request Description appears in the details on the View Attestation Request Status page.

Display Label:*

Request Description:*

Select the roles whose assignments will be verified during the attestation process.

Verify Assignments For:*

- All Roles
- Select Roles

Select the users who will verify the data during the attestation process. When selecting group(s) and role(s), select whether all members must verify the data, or only a single member in each group and role needs to verify the data to complete the process.

Attesters:*

User

- Every member of the group(s) and role(s) selected must attest to the data.
- A single member of each group and role selected must attest to the data.

Deadline:*

- Specify Duration (Weeks, Days, Hours)
Duration:* Weeks (From Now)
- Specify End Date
- No Expiration

Report Languages:*



Системные роли управления

- Администратор (Roles Module Administrator)
 - > Полный доступ ко всем элементам системы RBPM
- Менеджер (Roles Manager)
 - > создание и модификация ролей, управление ассоциациями
- Аудитор (Roles Auditor)
 - > просмотр отчётности
- Офицер безопасности (Security Officer)
 - > создание и управление правилами обработки ситуаций, назначения конфликтных ролей



Корпоративный справочник

The screenshot displays the Novell Identity Manager web interface. The main window shows a user profile for Elena Sunichuk. The interface includes a navigation menu on the left, a search bar, and a detailed view of the user's information.

Novell Identity Manager (29 Январь 2006 г.)

Welcome, Олег | Identity Self-Service | Requests & Approvals | Logout | Help

Information Management

Организационная структура предприятия

Lookup

Novell Identity Manager (29 Январь 2006 г.)

Welcome, Елена | Identity Self-Service | Requests & Approvals | Logout | Help

Information Management

Организационная структура

Мой профиль

Поиск по справочнику

Password Management

Забывшие пароли

Установка подсказок

Изменить пароль

General

Приветствуем

Детальный просмотр

Елена Суничук

[Edit Your Information](#)

[Send Identity Info](#)

[Display Organization Chart](#)

First Name:	Елена
Last Name:	Суничук
Title:	Менеджер по работе с партнёрами
Region:	офис 44
Email:	OSynichuk@novell.com
Manager:	Валерий Елизарьев
Telephone Number:	4940741



Механизмы синхронизации

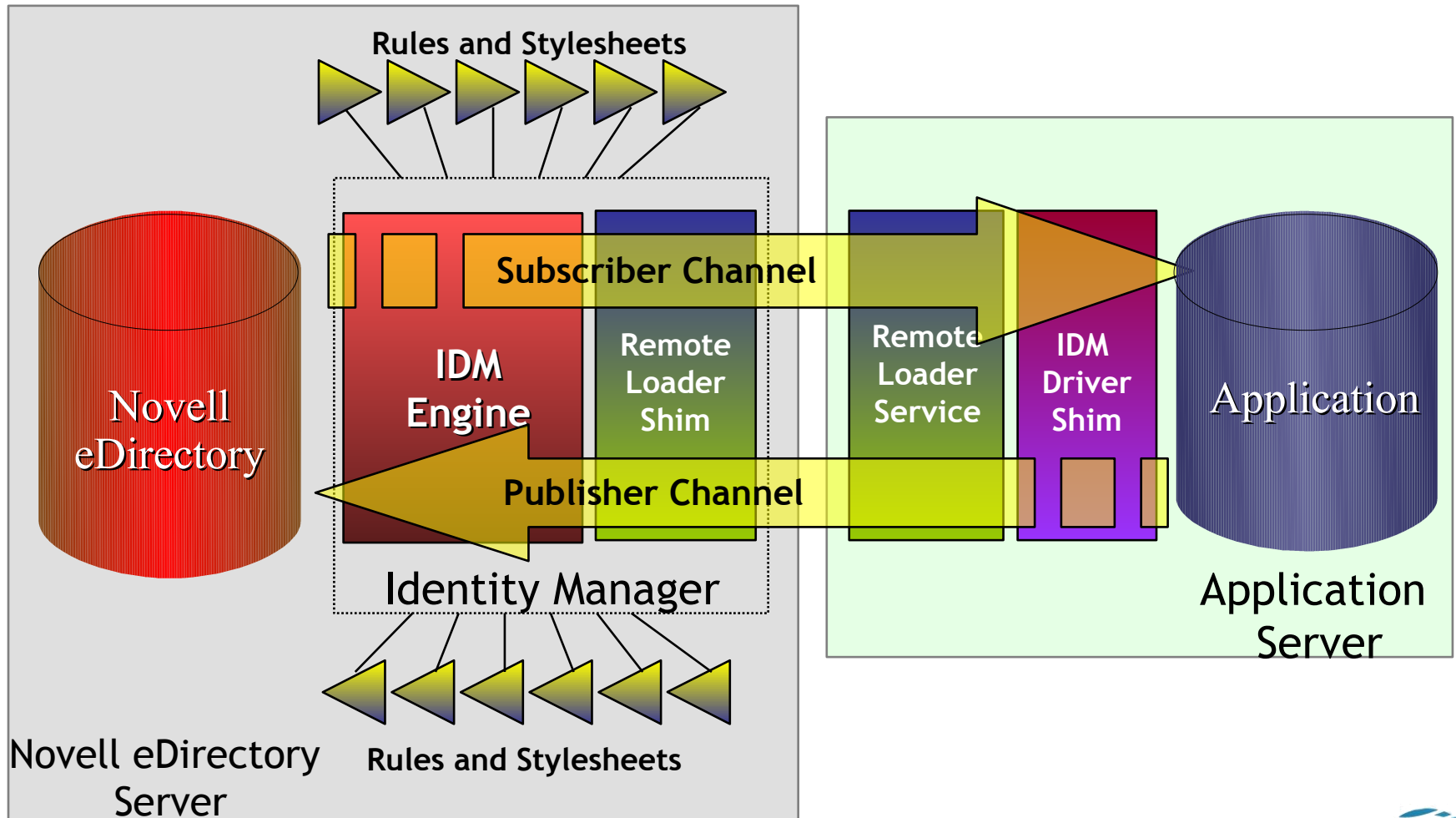
Метакаталог Identity Manager на базе Novell eDirectory



- В среднем в компании от 5 до 7 приложений, использующих собственные хранилища учётной информации пользователей.



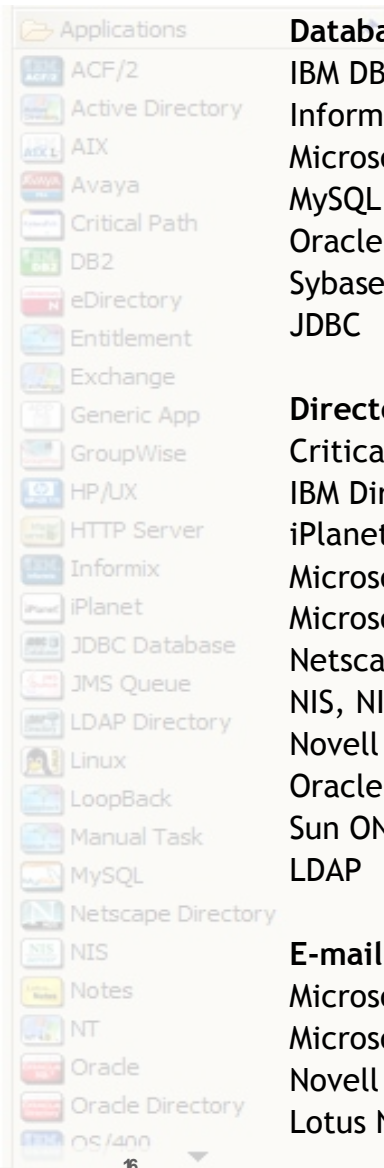
Механизмы синхронизации



Linux, Netware, Windows, Solaris



Поддержка огромного количества систем



Database

IBM DB2
Informix
Microsoft SQL Server
MySQL
Oracle
Sybase
JDBC

Directories

Critical Path InJoin Directory
IBM Directory Server (SecureWay)
iPlanet Directory Server
Microsoft Active Directory
Microsoft Windows NT Domains
Netscape Directory Server
NIS, NIS +
Novell NDS, eDirectory
Oracle Internet Directory
Sun ONE Directory Server
LDAP

E-mail systems

Microsoft Exchange 2000, 2003
Microsoft Exchange 5.5
Novell GroupWise
Lotus Notes

Enterprise applications

Baan
J.D.Edwards
Lawson
Oracle
Peoplesoft
SAP HR
SAP R/3 4.6
SAP Enterprise Systems
SAP Web Application Server
(Web AS) 6.20
Siebel

Enterprise message bus

BEA
IBM Websphere MQ
Open JMS
Oracle
JBOSS
Sun
TIBCO

Mainframe

RACF
ACF2
Top Secret

Midrange

OS/400 (AS/400)

Operating systems

Microsoft Windows NT 4.0
Microsoft Windows 2000/3
SUSE LINUX
Debian Linux
FreeBSD
Red Hat AS and ES
Red Hat Linux
HP-UX
IBM AIX
Solaris
UNIX Files - /etc/passwd

Other

Delimited Text
Remedy (for Help Desk)
SOAP
DSML
SPML
Schools Interoperability
Framework (SIF)

PBX

Avaya PBX



Управление паролями

Управление паролями

Набор функций, связанных с безопасностью паролей:

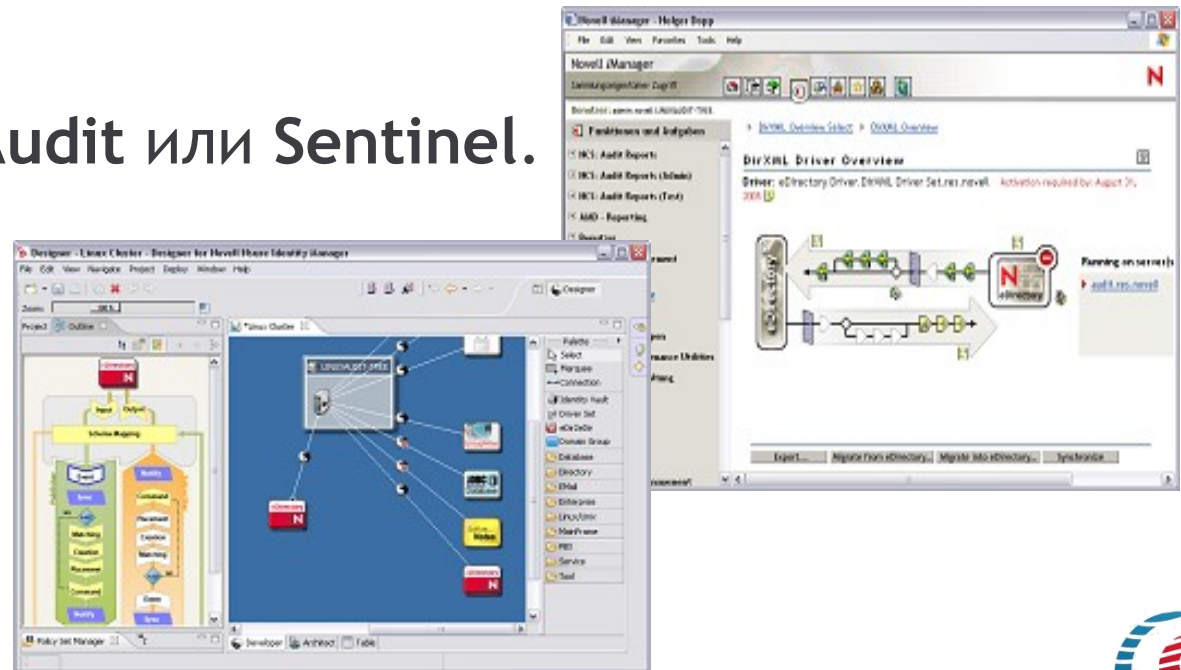
- Политика паролей масштаба всей системы
 - Установление политики паролей которая будет использоваться в каждой из подключенных систем
- Служба самообслуживания паролей
 - Используется сотрудниками для самостоятельного восстановления забытых паролей, сброса паролей и изменения паролей
- Распространение паролей
 - Определение связанных систем, которые получают общие пароли организации, в соответствии с политикой паролей
- Двухсторонняя синхронизация паролей
 - Управление собственной системой паролей в каждой подключенной системе обеспечивает согласованность



Проектирование,
администрирование,
мониторинг и аудит

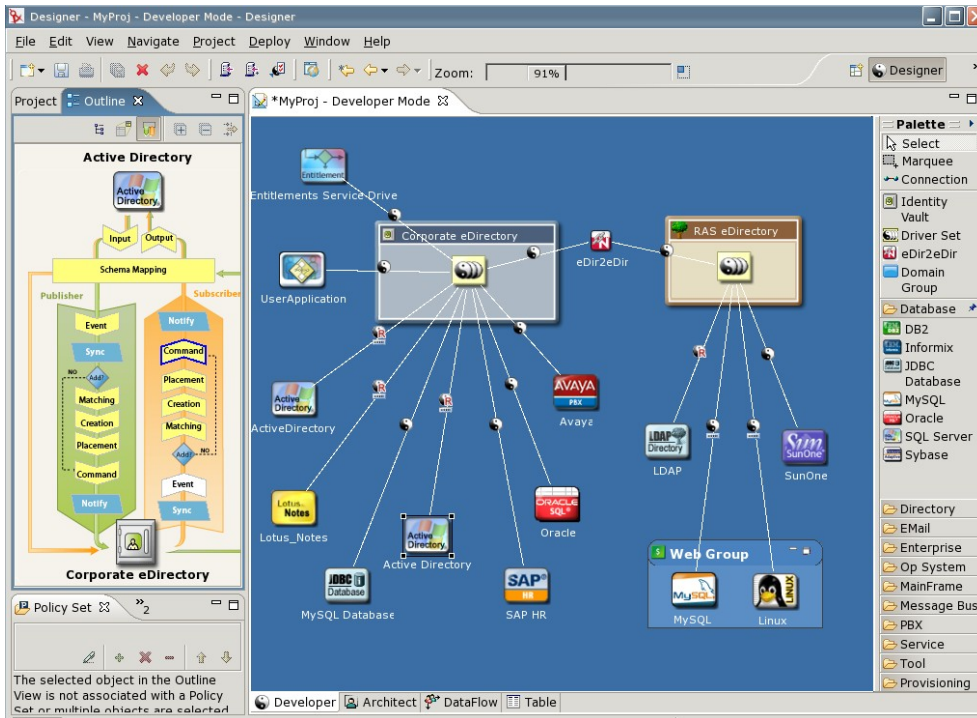
Инструментарий и продукты для управления

- Проектирование - **Designer for Identity Manager**.
- Администрирование, управление, мониторинг - **iManager**.
- Аудит - **Novell Audit** или **Sentinel**.



Проектирование мета-каталога

Novell Identity Designer



- Моделирование
- Разработка, настройка политик синхронизации
- Dataflow Modeler
- Средства взаимодействия с каталогами
- Отладка и симуляция
- Встроенный XML/XSLT редактор
- Инструменты развёртывания
- Подробная Справка
- Средства документирования проектов
- Поддержка Windows и Linux



Основные редакторы IDM Designer

- Редактор запросов согласования

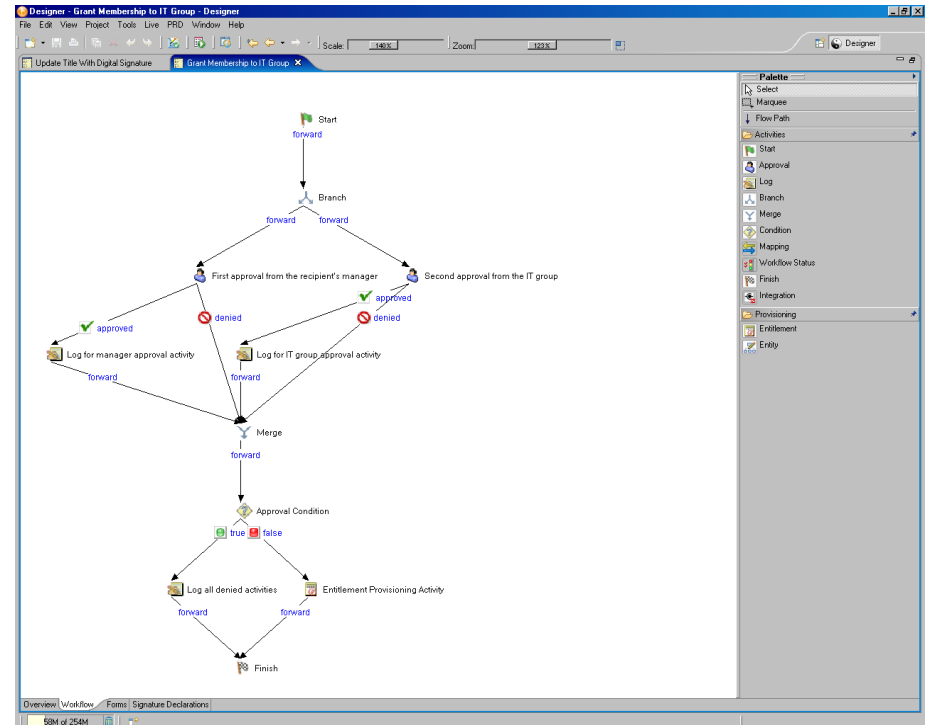
- Позволяет проводить визуальную разработку процедур согласования с последующим развёртыванием на сервер IDM

- Редактор форм

- Позволяет создавать нестандартные формы, используемые в процедурах согласования

- Редактор шаблонов оповещения

- Позволяет создавать TXT и HTML шаблоны оповещения, используемые на стадиях процедуры согласования



Автогенерация документации

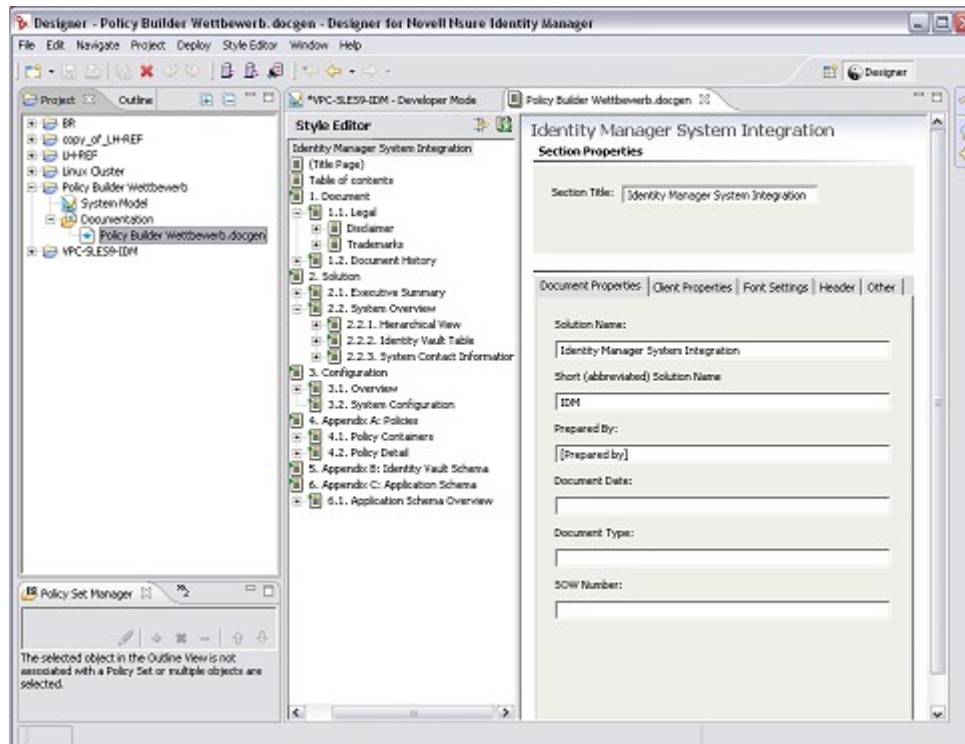


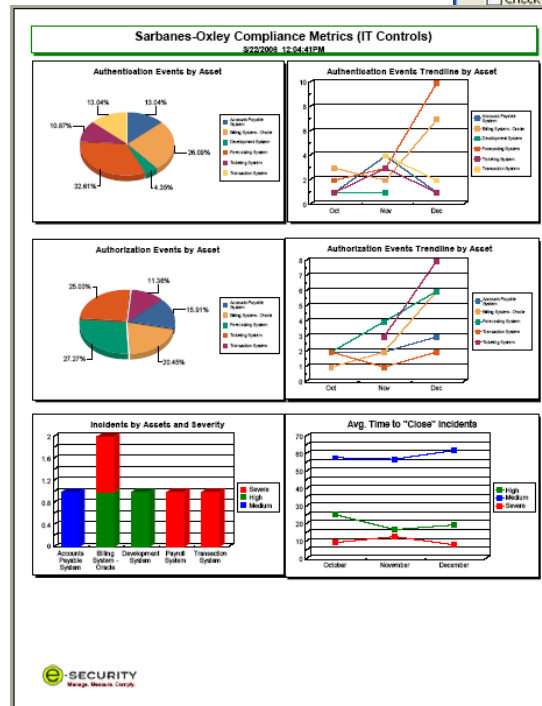
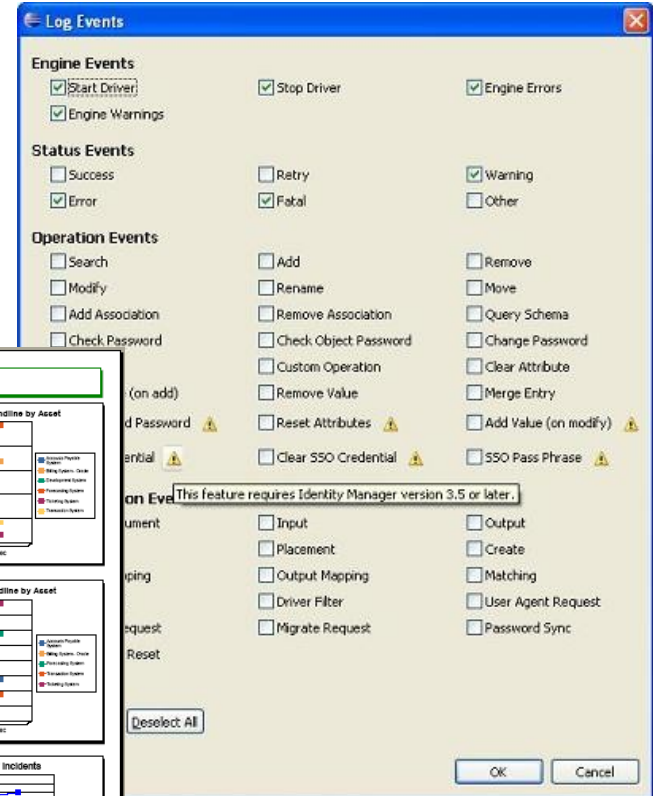
Table of contents

1. Document.....	4
1.1. Legal.....	4
1.2. Document History.....	5
2. Solution.....	6
2.1. Executive Summary.....	6
2.2. System Overview.....	7
2.2.1. Hierarchical View.....	7
2.2.2. Identity Vault Table.....	8
2.2.3. System Contact Information.....	8
3. Configuration.....	9
3.1. Overview.....	9
3.2. System Configuration.....	9
3.2.1. LINUXCLUSTER-TREE.....	9
3.2.1.1. DiXML Driver Set.....	13
3.2.1.1.1. CLtoAU.....	14
3.2.1.1.2. Delimited Text.....	24
3.2.1.1.3. Remove DiXML Trial Lic 2.0.....	28
3.2.2. eDirectory.....	30
3.2.3. RemoteApp.....	31
3.2.4. eDirectory.....	32
3.2.5. eDirectory.....	32
3.2.6. RemoteApp.....	32
3.2.7. eDirectory.....	32
3.2.8. LINUXAUDIT-TREE.....	33
3.2.8.1. DiXML Driver Set.....	37
3.2.8.1.1. Action Dumper.....	39
3.2.8.1.2. CA Driver.....	43
3.2.8.1.3. Common.....	47
3.2.8.1.4. eDirectory Driver.....	49
3.2.8.1.5. GroupWise.....	58
3.2.8.1.6. MSSQLAXI0G.....	64
3.2.8.1.7. Notes.....	68



Контроль событий управления

- Встроенный Event-Log
- Novell Audit Starter Pack
- Novell Sentinel



Системные требования, варианты поставки

Поддерживаемые ОС

Операционная система	32-бит ОС на 32-бит Processor	32-бит ОС на 64-бит Processor	64-бит ОС на 64-бит Processor
NetWare 6.5 SP6	Да	Да	N/A
OES 2 / 1.0 sp2 (NetWare)	Да	Да	N/A
Windows 2000 Server	Да	Да	N/A
Windows Server 2003	Да	Да	Только Password Sync
Red Hat Linux AS 3.0	Да	Да	N/A
Red Hat Linux AS 4.0	Да	Да	Да
SLES 8	Да	Да	Да
SLES 9	Да	Да	Да
SLES 10	N/A	Да	Да
OES 2 / 1.0 sp2 (Linux)	Да	Да	N/A
Solaris 9	N/A	N/A	Да
Solaris 10	N/A	N/A	Да
AIX 5.2L	N/A	N/A	Да
AIX 5.3	N/A	N/A	Да



Поддерживаемые платформы User Application

- Платформа ОС
 - OES 2 / 1.0 sp2
 - SLES 9 sp2, SLES 10
 - Windows 2003 sp1
 - Solaris 10
- JBoss Application Server 4.2 (поставляется в комплекте), IBM WebSphere 6.1
- MySQL 5.0.27 (поставляется в комплекте), Oracle 9i (9.2.0.1.4), Oracle 10g R2 (10.2.0.1.0), MS SQL 2005SP1, DB2 DV2 (9.1.0.0)



Поставляемые компоненты

Identity Manager 3.6

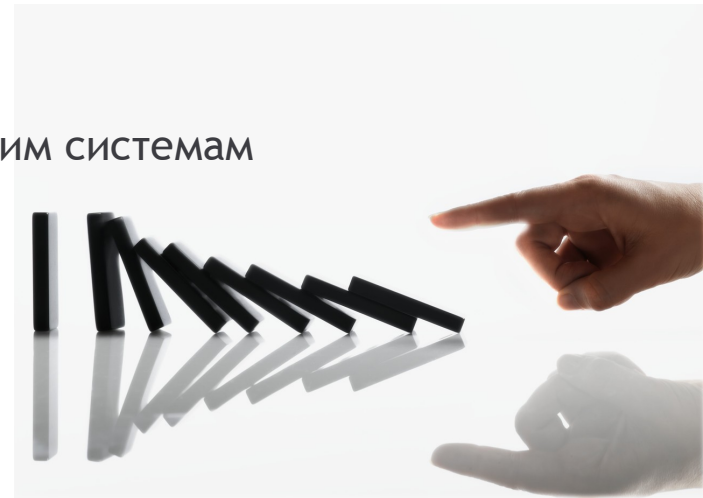
- > Ядро Identity Manager (Engine)
- > Базовый набор интеграционных модулей (Windows, Directory, Email)
- > Web-портал с функциональностью информационного справочника, самообслуживания

Roles Based Provisioning Module

- > Дополнительная функциональность Web-портала, автоматизирующая процедуры согласования доступа

Integration Modules

- > Набор коннекторов (драйверов) к другим системам



Что обеспечит Identity Manager?

- ✓ Без изменения существующих приложений
возможность централизованного ролевого управления пользователями в реальном времени
- ✓ Пользователи и группы различных систем будут автоматически синхронизироваться
- ✓ Процесс заказа ресурсов, режим согласования с делегирование полномочий
- ✓ Синхронизацию паролей
 - двунаправленная с AD, DomainNT, eDirectory, NIS+
- ✓ Автоматизацию обслуживания пароля
- ✓ Возможность быстрой разработки и развёртывания
- ✓ Аудит событий





Благодарю за внимание!

Контакты:

(056) 745 01 77

(067) 630 07 93

e-mail: info@systemintegrator.com.ua

www.systemintegrator.com.ua

Novell®

This is Your Open Enterprise™