AUTHORIZED DOCUMENTATION

Overview Guide

Novell® Identity Manager

4.0

October 15, 2010

www.novell.com

Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. Please refer to the International Trade Services (http://www.novell.com/company/policies/trade_services) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2008-2010 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide **7**

1 Identity Manager and Business Process Automation **9**

1.1 Data Synchronization . . . 10
1.2 Workflow . . . 13
1.3 Roles and Attestation . . . 14
1.4 Self-Service . . . 15
1.5 Auditing, Reporting, and Compliance . . . 16

2 Features of Identity Manager 4.0 **19**

3 Identity Manager Architecture **21**

3.1 Data Synchronization . . . 22
3.1.1 Components . . . 23
3.1.2 Key Concepts . . . 23
3.2 Workflow, Roles, Attestation, and Self-Service . . . 25
3.2.1 Components . . . 27
3.2.2 Key Concepts . . . 27
3.3 Auditing and Reporting . . . 28

4 Identity Manager Tools **31**

4.1 Analyzer . . . 32
4.2 Designer . . . 32
4.3 iManager . . . 33
4.4 Role Mapping Administrator . . . 34
4.5 Identity Reporting . . . 35

5 What's Next **37**

5.1 Planning an Identity Manager Solution . . . 37
5.2 Preparing Your Data for Synchronization . . . 37
5.3 Installing or Upgrading Identity Manager . . . 37
5.4 Configuring Identity Manager . . . 38
5.4.1 Synchronizing Data . . . 38
5.4.2 Mapping Roles . . . 38
5.4.3 Configuring the User Application . . . 38
5.4.4 Configuring Auditing, Reporting, and Compliance . . . 39
5.5 Administering Identity Manager . . . 39

About This Guide

This guide introduces you to Novell Identity Manager, a WorkloadIQ product that manages identity and access across physical, virtual, and cloud environments. This guide explains business issues that Identity Manager can help you solve while reducing costs and ensuring compliance. It also contains a technical overview of the Identity Manager components and tools you can use to create your Identity Manager solution. The guide is organized as follows:

- Chapter 1, “Identity Manager and Business Process Automation,” on page 9
- Chapter 2, “Features of Identity Manager 4.0,” on page 19
- Chapter 3, “Identity Manager Architecture,” on page 21
- Chapter 4, “Identity Manager Tools,” on page 31
- Chapter 5, “What’s Next,” on page 37

Audience

This guide is intended for administrators, consultants, and network engineers who require a high-level introduction to Identity Manager business solutions, technologies, and tools.

Documentation Updates

For the most recent version of this document, see the Identity Manager Documentation Web site (http://www.novell.com/documentation/idm40/index.html).

Additional Documentation

For documentation on Identity Manager drivers, see the Identity Manager Drivers Web site (http://www.novell.com/documentation/idm40drivers/index.html).

Identity Manager and Business Process Automation

1

The information in this section identifies some of the business processes you can automate through the implementation of a Novell Identity Manager system. If you are already aware of the business automation solutions provided by Identity Manager, you might want to skip to the technical introduction provided in Chapter 3, "Identity Manager Architecture," on page 21.

Managing identity needs is a core function of most businesses. For example, imagine that it's early Monday morning. You scroll down the list of requests in your queue:

- Jim Taylor's cell phone number has changed. You need to update it in the HR database and four other independent systems.
- Karen Hansen, just returning from an extended leave of absence, has forgotten her e-mail password. You need to help her retrieve or reset it.
- Jose Altimira just hired a new employee. You need to give the employee network access and an e-mail account.
- Ida McNamee wants access to the Oracle financial database, which requires you to get approval from three different managers.
- John Harris just moved from the Accounts Payable department to the Legal department. You need to give him access to the same resources as the other members of the Legal team and remove his access to Accounts Payable resources.
- Karl Jones, your own boss, saw a copy of Ida McNamee's request for access to the Oracle financial database and is concerned about the number of people with access. You need to generate a report for him that shows everyone who has access to the database.

You take a deep breath and start in on the first request, knowing that you'll be hard-pressed to keep up with all of the requests, let alone have time to finish the other projects assigned to you.

If this sounds like a common workday for you or someone in your organization, Identity Manager can help. In fact, the core Identity Manager capabilities, introduced in the following illustration, can help you automate all of these tasks and more. These capabilities—workflows, roles, attestation, self-service, auditing, and reporting—use multi-system data synchronization driven by your business policies to automate the processes involved in provisioning users and managing passwords, two of the most difficult and time-consuming duties of an IT organization.

Figure 1-1 *Identity Manager Core Capabilities*

The following sections introduce you to these Identity Manager capabilities and how they can help you successfully meet the identity needs of your organization:

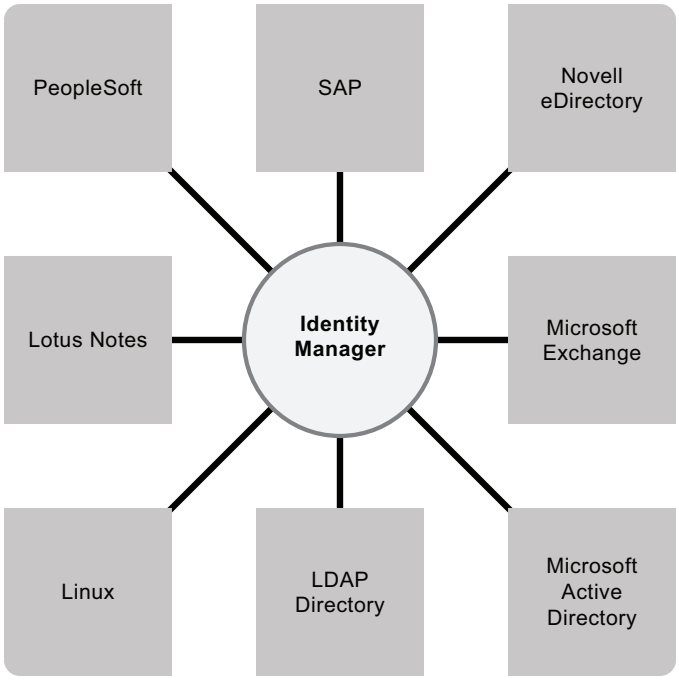
- Section 1.1, "Data Synchronization," on page 10
- Section 1.2, "Workflow," on page 13
- Section 1.3, "Roles and Attestation," on page 14
- Section 1.4, "Self-Service," on page 15
- Section 1.5, "Auditing, Reporting, and Compliance," on page 16

1.1 Data Synchronization

If your organization is like most, you have identity data stored in multiple systems. Or, you have identity data stored in one system that you could really use in another system. Either way, you need to be able to easily share and synchronize data between systems.

Identity Manager lets you synchronize, transform, and distribute information across a wide range of applications, databases, operating systems, and directories such as SAP, PeopleSoft, Salesforce, Microsoft SharePoint, Lotus Notes, Microsoft Exchange, Microsoft Active Directory, Novell eDirectory, Linux and UNIX, LDAP directories.

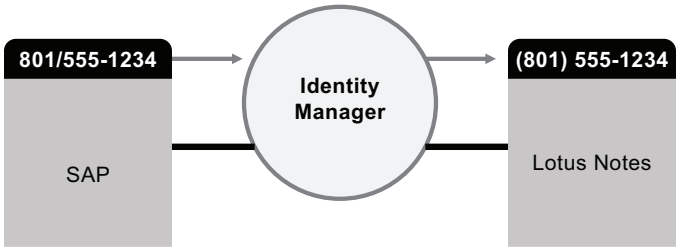
Figure 1-2 *Identity Manager Connecting Multiple Systems*



You control the flow of data among the connected systems. Among other things, you determine what data is shared, which system is the authoritative source for a piece of data, and how the data is interpreted and transformed to meet the requirements of other systems.

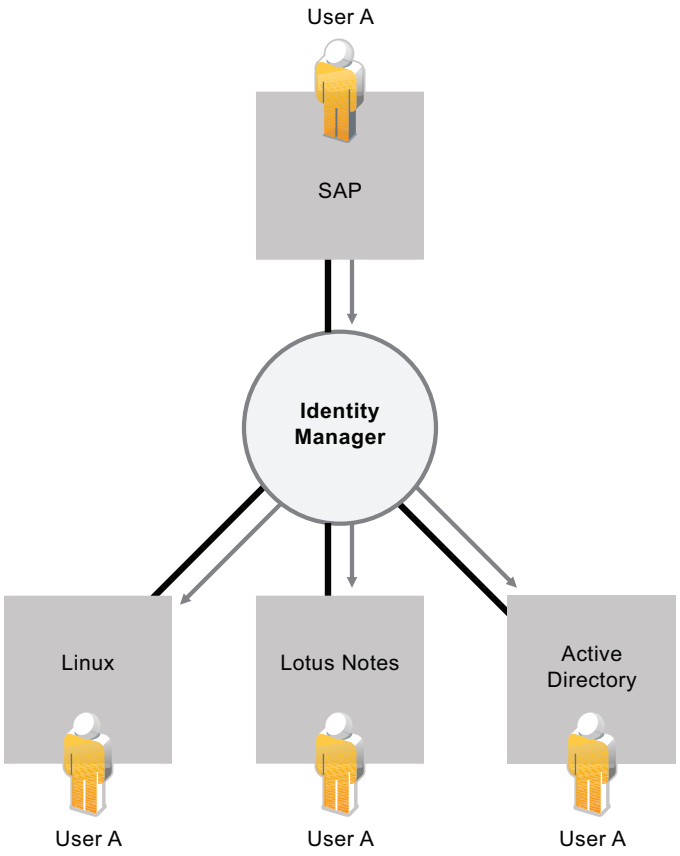
In the following diagram, the SAP HR database is the authoritative source for a user's telephone number. The Lotus Notes system also uses telephone numbers, so Identity Manager transforms the number into the required format and shares it with the Lotus Notes system. Whenever the telephone number changes in the SAP HR system, it is synchronized to the Lotus Notes system.

Figure 1-3 *Data Synchronization between Connected Systems*



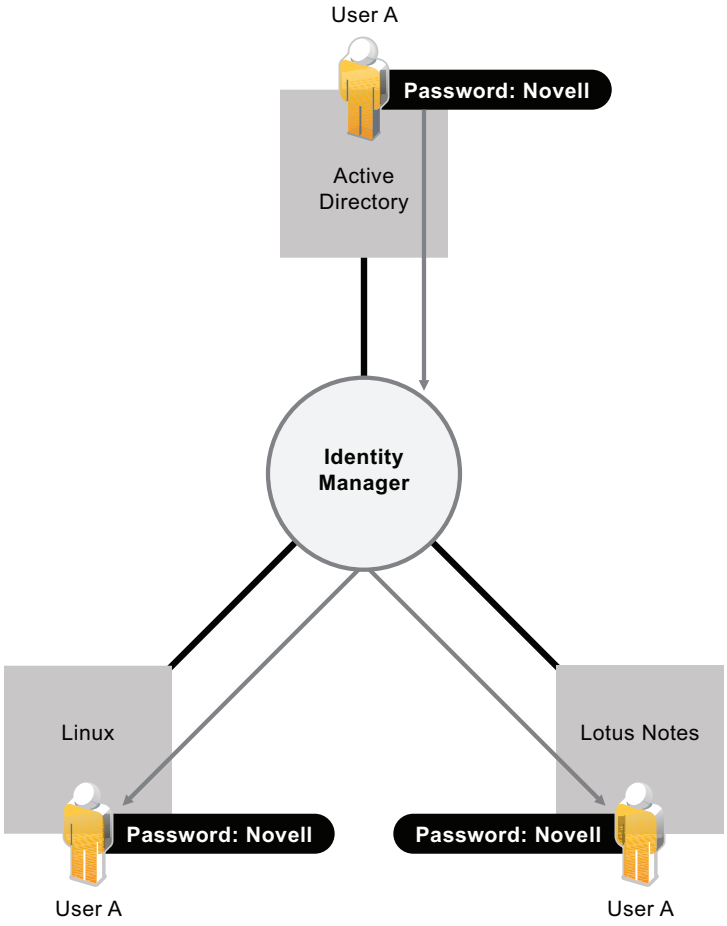
Managing data for existing users is just the beginning of the data synchronization capabilities of Identity Manager. In addition, Identity Manager can create new user accounts and remove existing accounts in directories such as Active Directory, systems such as PeopleSoft and Lotus Notes, and operating systems such as UNIX and Linux. For example, when you add a new employee to your SAP HR system, Identity Manager can automatically create a new user account in Active Directory, a new account in Lotus Notes, and a new account in a Linux NIS account management system.

Figure 1-4 *User Account Creation in Connected Systems*



As part of its data synchronization capability, Identity Manager can also help you synchronize passwords between systems. For example, if a user changes his or her password in Active Directory, Identity Manager can synchronize that password to Lotus Notes and Linux.

Figure 1-5 *Password Synchronization among Connected Systems*

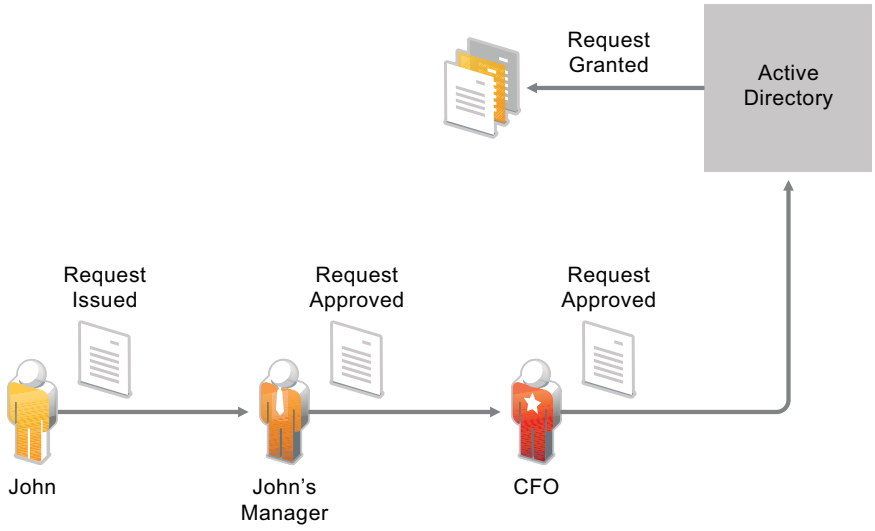


1.2 Workflow

More than likely, user access to many of the resources in your organization doesn't require anyone's approval. However, access to other resources might be restricted and require approval from one or more individuals.

Identity Manager provides workflow capabilities to ensure that your provisioning processes involve the appropriate resource approvers. For example, assume that John, who has already been provisioned with an Active Directory account, needs access to some financial reports through Active Directory. This requires approval from both John's immediate manager and the CFO. Fortunately, you've set up an approval workflow that routes John's request to his manager and, after approval from his manager, to the CFO. Approval by the CFO triggers automatic provisioning of the Active Directory rights needed by John to access and view the financial documents.

Figure 1-6 Approval Workflow for User Provisioning



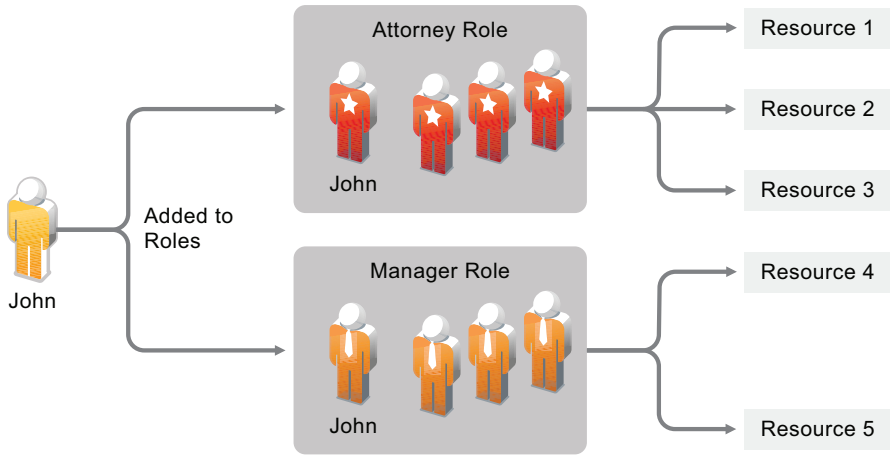
Workflows can be initiated automatically whenever a certain event occurs (for example, a new user is added to your HR system) or initiated manually through a user request. To ensure that approvals take place in a timely manner, you can set up proxy approvers and approval teams.

1.3 Roles and Attestation

Users often require access to resources based upon their roles in the organization. For example, a law firm's attorneys might require access to a different set of resources than the firm's paralegals.

Identity Manager lets you provision users based on their roles in the organization. You define the roles and make the assignments according to your organizational needs. When a user is assigned to a role, Identity Manager provisions the user with access to the resources associated with the role. If a user is assigned multiple roles, he or she receives access to the resources associated with all of the roles, as shown in the following illustration:

Figure 1-7 Role-Based Provisioning of Resources



You can have users automatically added to roles as a result of events that occur in your organization (for example, a new user being with the job title of Attorney added to your SAP HR database). If approval is required for a user to be added to a role, you can establish workflows to route role requests to the appropriate approvers. You can also manually assign users to roles.

In some cases, certain roles should not be assigned to the same person because the roles conflict. Identity Manager provides Separation of Duties functionality that lets you prevent users from being assigned to conflicting roles unless someone in your organization makes an exception for the conflict.

Because role assignments determine a user's access to resources within your organization, ensuring correct assignments is critical. Incorrect assignments could jeopardize compliance with both corporate and government regulations. Identity Manager helps you validate the correctness of your role assignments through an attestation process. Using this process, responsible individuals within your organization certify the data associated with roles:

- **User profile attestation:** Selected users attest to their own profile information (first name, last name, title, department, e-mail, and so forth) and correct any incorrect information. Accurate profile information is essential to correct role assignments.
- **Separation of Duties violation attestation:** Responsible individuals review a Separation of Duties violation report and attest to the accuracy of the report. The report lists any exceptions that allow a user to be assigned conflicting roles.
- **Role assignment attestation:** Responsible individuals review a report listing selected roles and the users, groups, and roles assigned to each role. The responsible individuals must then attest to the accuracy of the information.
- **User assignment attestation:** Responsible individuals review a report listing selected users and the roles to which they are assigned. The responsible individuals must then attest to the accuracy of the information.

These attestation reports are designed primarily to help you ensure that role assignments are accurate and that there are valid reasons for allowing exceptions for conflicting roles.

1.4 Self-Service

You probably have business managers and departments clamoring to manage their own users' information and access needs instead of relying on you or your staff. How many times have you heard "Why can't I change my own cell phone number in our corporate directory?" or "I'm in the Marketing department. Why do I have to call the Help Desk to get access to the Marketing Information database?"

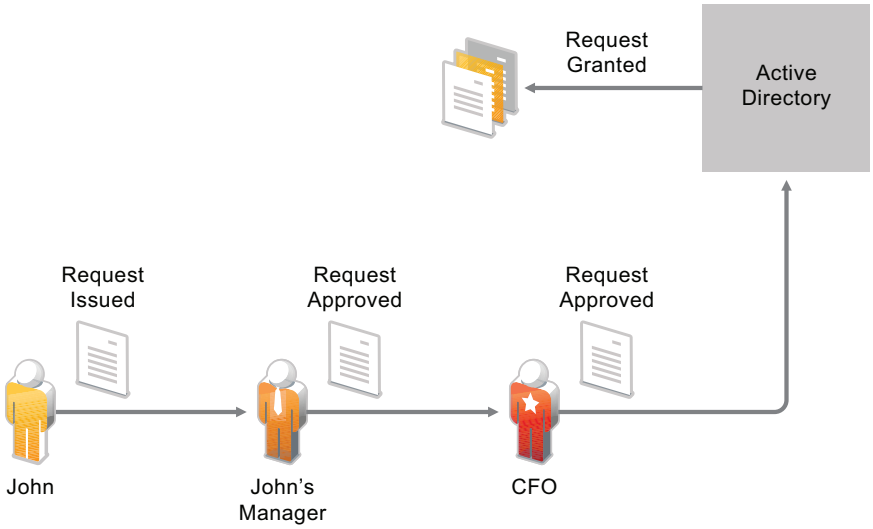
With Identity Manager, you can delegate administrative duties to the people who should be responsible for them. For example, you can enable individual users to:

- Manage their own personal data in the corporate directory. Rather than having you change a cell phone number, they can change it in one place and have it changed in all the systems you've synchronized through Identity Manager.

- Change their passwords, set up a hint for forgotten passwords, and set up challenge questions and responses for forgotten passwords. Rather than asking you to reset a password because they've forgotten it, they can do it themselves after receiving a hint or responding to a challenge question.
- Request access to resources such as databases, systems, and directories. Rather than calling you to request access to an application, they can select the application from a list of available resources.

In addition to self-service for individual users, Identity Manager provides self-service administration for functions (management, Help Desk, and so forth) that are responsible for assisting, monitoring, and approving user requests. For example, consider the scenario used in Section 1.2, "Workflow," on page 13 and shown below.

Figure 1-8 *Provisioning Workflow with Self-Service*



Not only does John use the Identity Manager self-service capability to request access to the documents he needs, but John's manager and the CFO use the self-service capability to approve the request. The established approval workflow allows John to initiate and monitor the progress of his request and allows John's manager and CFO to respond to his request. Approval of the request by John's manager and the CFO triggers the provisioning of the Active Directory rights needed by John to access and view the financial documents.

1.5 Auditing, Reporting, and Compliance

Without Identity Manager, provisioning users can be a tedious, time-consuming, and costly effort. That effort, however, can pale in comparison to verifying that your provisioning activities have complied with your organization's policies, requirements, and regulations. Do the right people have access to the right resources? Are the wrong people shut out of those same resources? Does the employee who started yesterday have access to the network, his e-mail, and the six other systems required for his job? Has the access been canceled for the employee who left last week?

With Identity Manager, you can relax in your knowledge that all of your user provisioning activities, past and present, are being tracked and logged for auditing purposes. Identity Manager contains an intelligent repository of information about the actual state and the desired state of the Identity Vault

and the managed systems within your organization. By querying the warehouse, you can retrieve all of the information you need to ensure that your organization is in full compliance with relevant business laws and regulations.

The warehouse gives you a 360-degree view of your business entitlements, providing the knowledge you need to see the past and present state of authorizations and permissions granted to identities in your organization. With this knowledge, you can answer even the most sophisticated Governance Risk and Compliance (GRC) queries.

Identity Manager contains predefined reports that let you perform queries against the Identity Information Warehouse to demonstrate compliance for business, IT, and corporate policies. You can also create custom reports if the predefined reports don't meet your needs.

Features of Identity Manager 4.0

2

Novell Identity Manger 4.0 provides an intelligent identity framework that leverages your existing IT assets and new computing models like Software as a Service (SaaS) by reducing cost and ensuring compliance across physical, virtual, and cloud environments. With Novell Identity Manager solutions, you can make sure that your business has the most current user identity information. You can retain control at the enterprise level by managing, provisioning, and deprovisioning identities within the firewall and extending to the cloud. Identity Manager can also help you to extend your compliance management to the cloud.

Identity Manager 4.0 offers you an integrated identity management, roles management, cutting-edge reporting, and package management capabilities for pre-configuring and customizing Identity Manager driver policies. You can also apply security policies across various system domains. It allows you to manage the user life cycle in growing regulatory requirements, and applies more granular protection with more strategic user provisioning to satisfy the growing security concerns within the firewall or in the cloud environment. The intelligent identity framework helps you use your existing infrastructure with new computing models like SaaS.

Novell Identity Manager 4.0: A Complete End-to-End Solution

- **Comprehensive Out-of-the-Box Reporting:** The integrated reporting module of the Novell Identity Manager 4.0 product suite enhances visibility into compliance across in-house and cloud deployments. The new reporting features let you see a user's identity state and access rights, or report on a user's actions and provisioning history. For more information, see the *Identity Reporting Module Guide*.
- **Enhanced Integration:** For creating a new Identity Manager solution where all of the components reside on the same server, Novell Identity Manager 4.0 introduces an integrated installer that simplifies the installation process and lets you set up your system more quickly. Instead of installing each Identity Manager component separately, you use the integrated installer to install all of the components in one operation. For more information, see the *Identity Manager 4.0 Integrated Installation Guide*.
- **Package Management:** Identity Manager 4.0 introduces a new concept called Package Management. This is a system for creating, distributing, and consuming high-quality building blocks of Identity Manager policy content. For more information about Identity Manager packages, see the *Configuring Packages* in the *Designer 4.0 for Identity Manager 4.0 Administration Guide*.
- **Cloud-Ready Drivers:** Identity Manager 4.0 offers several drivers for out-of-the-box integration with SaaS. The drivers give you seamless integration with SaaS and the hosted solution by providing capabilities such as provisioning, deprovisioning, request/approval processes, password changes, identity profile updates, and reporting. New SharePoint and Salesforce.com drivers help your enterprise identities to integrate with cloud applications. For more information about cloud-ready drivers, see the *Identity Manager 4.0 Driver for Salesforce.com Implementation Guide* and the *Identity Manager 4.0 Driver for SharePoint Implementation Guide*.
- **Embedded Identity Vault:** The new architecture of Novell Identity Manager 4.0 products includes an optional built-in Identity Vault so you don't need to create and manage a separate directory structure for identity purposes. In addition, the Novell Identity Manager 4.0 family of

products includes drivers to easily integrate the Identity Vault with other repositories of identity information in your enterprise, such as Active Directory or various databases. For more information, see the *Identity Manager 4.0 Integrated Installation Guide*.

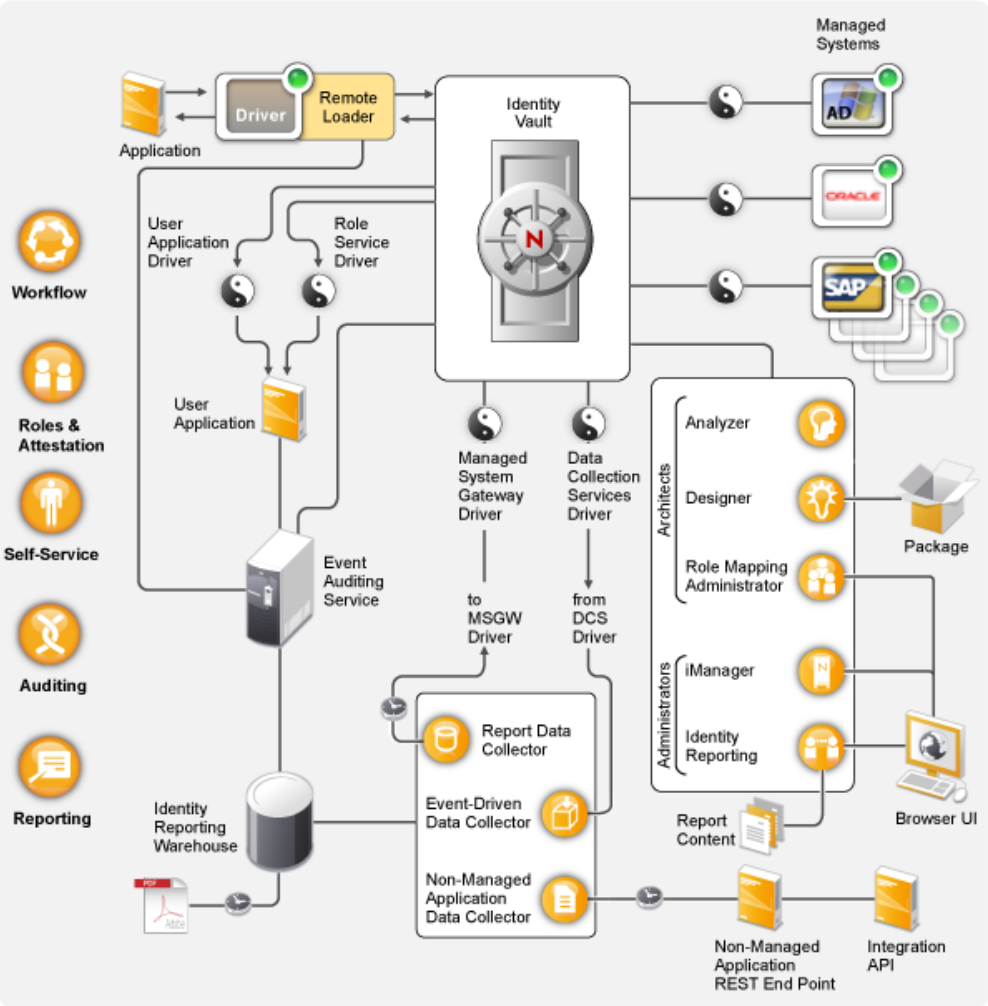
- **Simplified Identity and Roles Management:** The Novell Identity Manager 4.0 product suite simplifies the integration of different role repositories into one consolidated location, which means you don't need to manage separate sources of identity information. By using the Role Mapping Administrator with its new intuitive interface, you can even map third-party roles and profiles to Novell Identity Manager 4.0. For more information, see the *Novell Identity Manager Role Mapping Administrator 2.0 User Guide*.
- **Enhanced Tools:** Designer is an important tool that includes the business and technical information to create an Identity Manager solution that fits your needs. Several enhancements have been made to Designer 4.0. See the list of Designer enhancements at *What's New* (http://www.novell.com/documentation/designer40/resources/whatsnew/index.html). For information about Designer features and administration, see the *Designer 4.0 for Identity Manager 4.0 Administration Guide*. In addition, Identity Manager contains a tool to help you simplify the process of analyzing and cleaning your data. For more information, see the *Analyzer 1.2 for Identity Manager Administration Guide*.

Identity Manager Architecture

3

The following diagram shows the high-level architecture components that provide the Novell Identity Manager capabilities introduced in Chapter 1, "Identity Manager and Business Process Automation," on page 9: data synchronization, workflow, roles, attestation, self-service, and auditing/reporting.

Figure 3-1 *Identity Manager High-Level Architecture*



Each of the components is introduced in the following sections:

- Section 3.1, "Data Synchronization," on page 22
- Section 3.2, "Workflow, Roles, Attestation, and Self-Service," on page 25
- Section 3.3, "Auditing and Reporting," on page 28

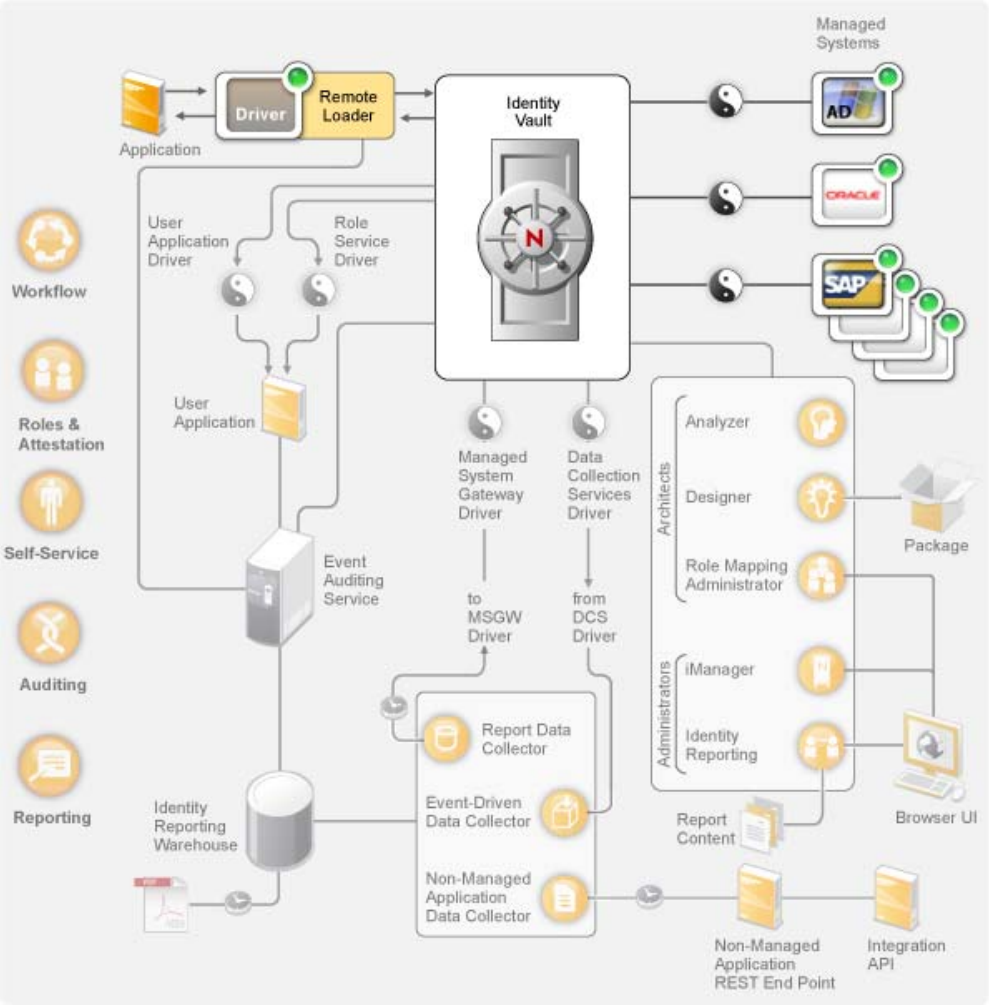
3.1 Data Synchronization

Data synchronization provides the foundation for automating business processes. In its simplest form, data synchronization is the movement of data from the location where a data item is changed to other locations where the data item is needed. For example, if an employee's phone number is changed in a company's Human Resources system, the change would automatically appear in all other systems that store the employee's phone number.

Identity Manager is not limited to the synchronization of identity data. Identity Manager can synchronize any type of data stored in the connected application or in the Identity Vault.

Data synchronization, including password synchronization, is provided by the five base components of the Identity Manager solution: the Identity Vault, Identity Manager engine, drivers, Remote Loader, and connected applications. These components are shown in the following diagram.

Figure 3-2 *Identity Manager Architecture Components*



The following sections provide descriptions of each of these components and explain the concepts you should understand to effectively synchronize data among systems in your organization:

- Section 3.1.1, "Components," on page 23
- Section 3.1.2, "Key Concepts," on page 23

3.1.1 Components

Identity Vault: The Identity Vault serves as a metadirectory of the data you want synchronized between applications. For example, data synchronized from a PeopleSoft system to Lotus Notes is first added to the Identity Vault and then sent to the Lotus Notes system. In addition, the Identity Vault stores information specific to Identity Manager, such as driver configurations, parameters, and policies. Novell eDirectory is used for the Identity Vault.

Identity Manager Engine: When data changes in the Identity Vault or a connected application, the Identity Manager engine processes the changes. For events that occur in the Identity Vault, the engine processes the changes and issues commands to the application via the driver. For events that occur in the application, the engine receives the changes from the driver, processes the changes, and issues commands to the Identity Vault. The Identity Manager engine is also referred to as the Metadirectory engine.

Driver: Drivers connect to the applications whose identity information you want to manage. A driver has two basic responsibilities: reporting data changes (events) in the application to the Identity Manager engine, and carrying out data changes (commands) submitted by the Identity Manager engine to the application.

Remote Loader: Drivers must be installed and run on the same server as the application to which they are connecting. If the application is located on the same server as the Identity Manager engine, all you need to do is install the driver to that server. However, if the application is not located on the same server as the Identity Manager engine (in other words, it is remote to the engine's server rather than local), you must install the driver and the Remote Loader to the application's server. The Remote Loader loads the driver and communicates with the Identity Manager engine on behalf of the driver.

Application: A system, directory, database, or operating system that a driver connects to. The application must provide APIs that a driver can use to determine application data changes and effect application data changes. Applications are frequently referred to as *connected systems*.

3.1.2 Key Concepts

Channels: Data flows between the Identity Vault and a connected system along two separate *channels*. The *Subscriber channel* provides data flow from the Identity Vault to a connected system; in other words, the connected system subscribes to data from the Identity Vault. The *Publisher channel* provides data flow from a connected system to the Identity Vault; in other words, the connected system publishes data to the Identity Vault.

Data Representation: Data flows through a channel as *XML documents*. An XML document is created when a change occurs in the Identity Vault or the connected system. The XML document is passed to the Identity Manager engine, which processes the document through the set of filters and policies associated with the driver's channel. When all processing has been applied to the XML

document, the Identity Manager engine uses the document to initiate the appropriate changes to the Identity Vault (Publisher channel), or the driver uses the document to initiate the appropriate changes in the connected system (Subscriber channel).

Data Manipulation: As XML documents flow through a driver channel, the document data is affected by the *policies* associated with the channel.

Policies are used for many things, including changing data formats, mapping attributes between the Identity Vault and the connected system, conditionally blocking the flow of data, generating e-mail notifications, and modifying the type of data change.

Data Flow Control: *Filters*, or *filter policies*, control the flow of data. Filters specify which items of data are synchronized between the Identity Vault and a connected system. For example, user data is typically synchronized between systems. Therefore, the user data is listed in the filter for most connected systems. However, printers are generally not of interest to most applications, so printer data does not appear in the filter for most connected systems.

Each relationship between the Identity Vault and a connected system has two filters: a filter on the Subscriber channel that controls data flow from the Identity Vault to the connected system, and a filter on the Publisher channel that controls data flow from the connected system to the Identity Vault.

Authoritative Sources: Most items of data associated with identity have a conceptual owner. The owner of a data item is considered the *authoritative source* for the item. In general, only the authoritative source for a data item is allowed to make changes to the data item.

For example, the corporate e-mail system is generally considered the authoritative source for an employee's e-mail address. If an administrator of the corporate white pages directory changes an employee's e-mail address in that system, the change has no effect on whether the employee actually receives e-mail at the changed address because the change must be made to the e-mail system to be effective.

Identity Manager uses filters to specify authoritative sources for an item. For example, if the filter for the relationship between the PBX system and the Identity Vault allows an employee's telephone number to flow from the PBX system into the Identity Vault but not from the Identity Vault to the PBX system, then the PBX system is the authoritative source for the telephone number. If all other connected system relationships allow the telephone number to flow from the Identity Vault to the connected systems, but not vice versa, the net effect is that the PBX system is the only authoritative source for employee telephone numbers in the enterprise.

Automated Provisioning: Automated provisioning refers to Identity Manager's ability to generate user provisioning actions other than the simple synchronization of data items.

For example, in a typical Identity Manager system where the Human Resource database is the authoritative source for most employee data, the addition of an employee to the HR database triggers the automatic creation of a corresponding account in the Identity Vault. The creation of the Identity Vault account in turn triggers the automatic creation of an e-mail account for the employee in the e-mail system. Data used to provision the e-mail system account is obtained from the Identity Vault and might include employee name, location, telephone number, and so forth.

The automatic provisioning of accounts, access, and data can be controlled in various ways, including:

- **Data item values:** For example, the automatic creation of an account in the access databases for various buildings can be controlled by a value in an employee's location attribute.

- **Approval workflows:** For example, the creation of an employee in the finance department can trigger an automatic e-mail to the finance department head requesting approval for a new employee account in the finance system. The finance department head is directed by the e-mail to a Web page where the department head approves or rejects the request. Approval can then trigger the automated creation of an account for the employee in the finance system.
- **Role assignments:** For example, an employee is given the role of Accountant. Identity Manager provisions the employee with all accounts, access, and data assigned to the Accountant role, either through system workflows (no human intervention), human approval flows, or a combination of both.

Entitlements: An entitlement represents a resource in a connected system, such as an account or a group membership. When a user meets the criteria established for an entitlement in a connected system, Identity Manager processes an event for the user that results in the user being granted access to the resource. This, of course, requires that all of the policies be in place to enable access to the resource. For example, if a user meets the criteria for an Exchange account in Active Directory, the Identity Manager engine processes the user through the set of Active Directory driver policies that provide an Exchange account.

The key benefit of entitlements is that you can define the business logic for access to a resource in one entitlement rather than multiple driver policies. For example, you can define an Account entitlement that gives a user an account in four connected systems. The decision to provide the user with an account is determined by the entitlement, which means that policies for each of the four drivers do not need to include the business logic. Instead, the policies only need to provide the mechanism for granting the account. If you need to make a business logic change, you change it in the entitlement instead of in each driver.

Jobs: For the most part, Identity Manager acts in response to data changes or user requests. For example, when a piece of data changes in one system, Identity Manager changes the corresponding data in another system. Or, when a user requests access to a system, Identity Manager initiates the appropriate processes (workflows, resource provisioning, and so forth) to provide the access.

Jobs enable Identity Manager to perform actions not initiated by data changes or user requests. A job consists of configuration data stored in the Identity Vault and a corresponding piece of implementation code. Identity Manager includes predefined jobs that perform such actions as starting or stopping drivers, sending e-mail notifications of expiring passwords, and checking the health status of drivers. You can also implement custom jobs to perform other actions; a custom job requires you (or a developer/consultant) to create the code required to perform the desired actions.

Work Orders: Typically, changes to data in the Identity Vault or a connected application are immediately processed. Work orders enable you to schedule tasks to be performed on a specific date and time. For example, a new employee is hired but is not scheduled to start for a month. The employee needs to be added to the HR database, but should not be granted access to any corporate resources (e-mail, servers, and so forth) until the start date. Without a work order, the user would be granted access immediately. With work orders implemented, a work order is created that initiates account provisioning only on the start date.

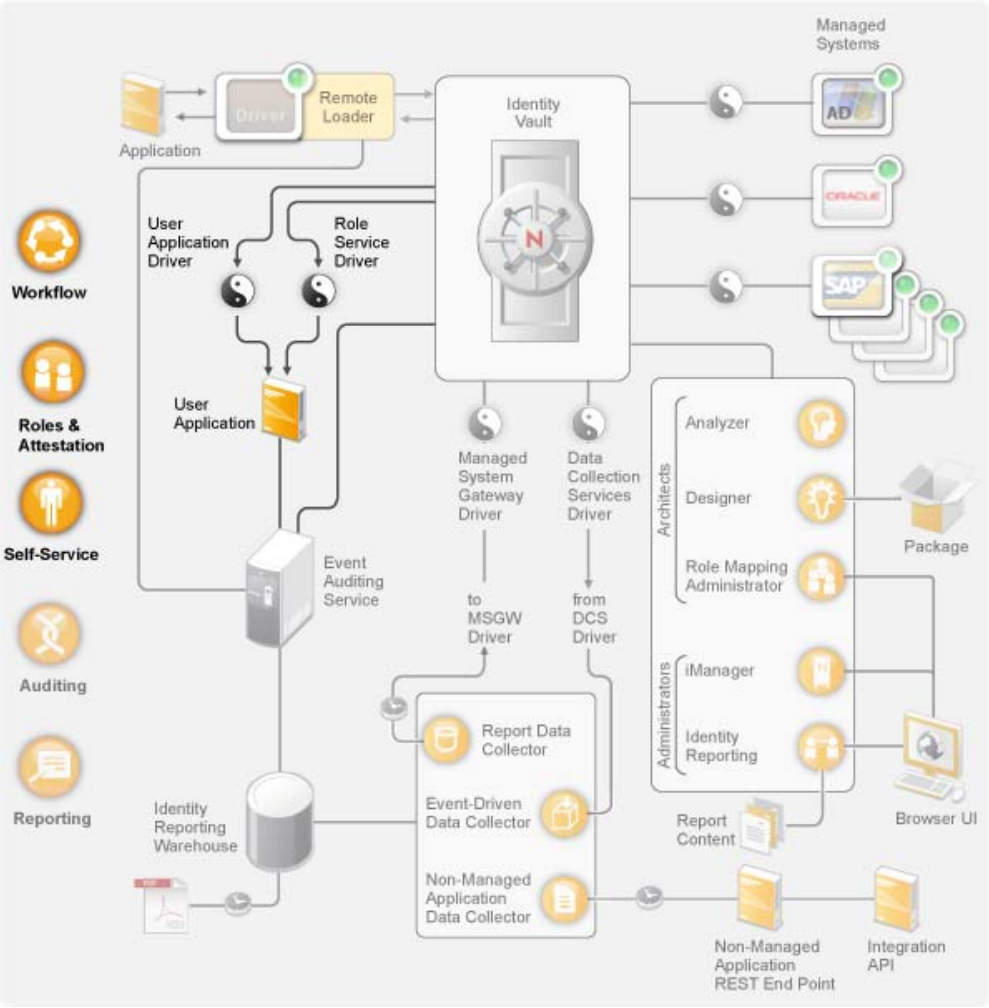
3.2 Workflow, Roles, Attestation, and Self-Service

Identity Manager provides a specialized application, the User Application, that provides approval workflows, role assignments, attestation, and identity self-service.

The standard User Application is included with Identity Manager. The standard version provides password self-service to help users remember or reset forgotten passwords, organization charts to manage user directory information, user management functionality that enables creation of users in the Identity Vault, and basic identity self-service such as management of user profile information.

The User Application Roles Based Provisioning Module is a part of Identity Manager 4.0 Advanced Edition. A standard User Application with advanced self-service, approval workflow, roles-based provisioning, Separation of Duties constraints, and attestation capabilities is included. The Identity Manager 4.0 Advanced Edition contains both the standard and the roles based provisioning module capabilities.

Figure 3-3 *Identity Manager User Application*



The following sections provide descriptions of each of these components and explain the concepts you should understand to effectively implement and manage the components:

- Section 3.2.1, “Components,” on page 27
- Section 3.2.2, “Key Concepts,” on page 27

3.2.1 Components

User Application: The User Application is a browser-based Web application that gives users and business administrators the ability to perform a variety of identity self-service and roles provisioning tasks, including managing passwords and identity data, initiating and monitoring provisioning and role assignment requests, managing the approval process for provisioning requests, and verifying attestation reports. It includes the workflow engine that controls the routing of requests through the appropriate approval process.

User Application Driver: The User Application driver stores configuration information and notifies the User Application whenever changes occur in the Identity Vault. It can also be configured to allow events in the Identity Vault to trigger workflows and to report success or failure of a workflow's provisioning activity to the User Application so that users can view the final status of their requests.

Role and Resource Service Driver: The Role and Resource Service driver manages all role and resource assignments, starts workflows for role and resource assignment requests that require approval, and maintains indirect role assignments according to group and container memberships. The driver also grants and revokes entitlements for users based on their role memberships, and performs cleanup procedures for requests that have been completed.

3.2.2 Key Concepts

Workflow-based Provisioning: Workflow-based provisioning provides a way for users to request access to resources. A provisioning request is routed through a predefined workflow that might include approval from one or more individuals. If all approvals are granted, the user receives access to the resource. Provisioning requests can also be initiated indirectly in response to events occurring in the Identity Vault. For example, adding a user to a group might initiate a request to have the user granted access to a specific resource.

Roles Based Provisioning: Roles based provisioning provides a way for users to receive access to specific resources based upon the roles assigned to them. Users can be assigned one or more roles. If a role assignment requires approval, the assignment request starts a workflow.

Separation of Duties: To prevent users from being assigned to conflicting roles, the User Application Roles Based Provisioning Module provides a Separation of Duties feature. You can establish Separation of Duties constraints that define which roles are considered to be in conflict. When roles conflict, Separation of Duties approvers can approve or deny any exceptions to the constraints. Approved exceptions are recorded as Separation of Duties violations and can be reviewed through the attestation process described below.

Roles Management: Management of roles must be done by individuals assigned to the Roles Module Administrator and Roles Manager system roles.

The Roles Module Administrator creates new roles, modifies existing roles, and removes roles; modifies relationships between roles; grants or revokes role assignments for users; and creates, modifies, and removes Separation of Duties constraints.

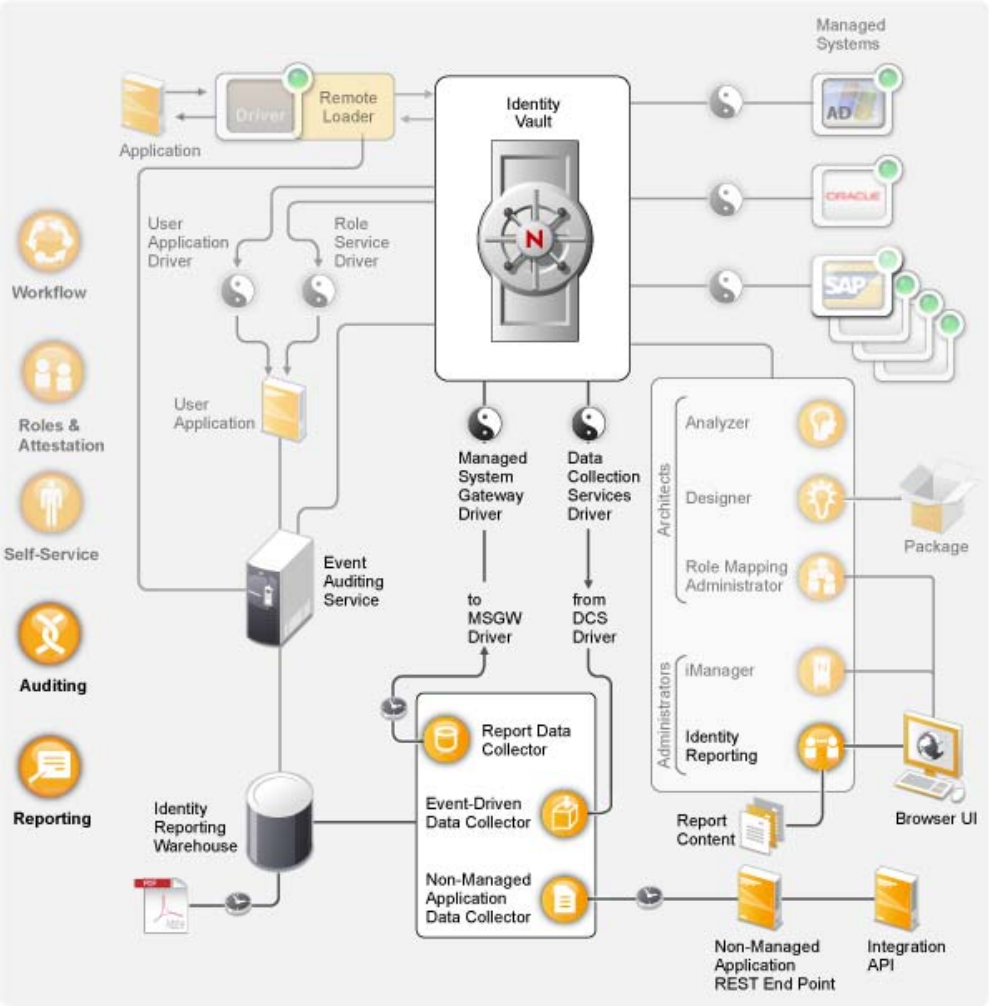
The Roles Manager can do the same things as the Roles Module Administrator with the exception of managing Separation of Duties constraints, configuring the Roles system, and running all reports. The Roles Module Administrator has unlimited scope within the Roles system, but the Roles Manager scope is limited to specifically-designated users, groups, and roles.

Attestation: Role assignments determine a user's access to resources within your organization, and incorrect assignments could jeopardize compliance with both corporate and government regulations. Identity Manager helps you validate the correctness of role assignments through an attestation process. Using this process, individual users can validate their own profile information and Roles Managers can validate role assignments and Separation of Duties violations.

3.3 Auditing and Reporting

Auditing and reporting is provided by the Identity Reporting Module, a new feature for Identity Manager 4.0, as shown in the following diagram.

Figure 3-4 *Identity Manager Auditing and Reporting*



The Identity Reporting Module generates reports that show critical business information about various aspects of your Identity Manager configuration, including information collected from Identity Vaults and managed systems such as Active Directory or SAP. The Identity Reporting Module uses the following components to manage the data:.

Event Auditing Service: A service that captures log events associated with actions performed in the reporting module, such as the import, modification, deletion, or scheduling of a report. The Event Auditing Service (EAS) captures log events associated with actions performed within the Roles Based Provisioning Module (RBPM) and the Role Mapping Administrator (RMA).

Identity Information Warehouse: Repository for the following type of information:

- Report management information (such as report definitions, report schedules, and completed reports), database views used for reporting, and configuration information.
- Identity data collected by the Report Data Collector, Event-Driven Data Collector, and the Non-Managed Application Data Collector.
- Auditing data, which includes events collected by the Event Auditing Service.

The Identity Information Warehouse stores its data in the Security Information and Event Management (SIEM) database.

Data Collection Service: A service that collects information from various sources within an organization. The Data Collection Service includes three subservices:

- **Report Data Collector:** Uses a pull design model to retrieve data from one or more Identity Vault data sources. The collection runs on a periodic basis, as determined by a set of configuration parameters. To retrieve the data, the collector calls the Managed System Gateway driver.
- **Event-Driven Data Collector:** Uses a push design model to gather event data captured by the Data Collection Service driver.
- **Non-Managed Application Data Collector:** Retrieves data from one or more non-managed applications by calling a REST end point written specifically for each application. Non-managed applications are applications within your enterprise that are not connected to the Identity Vault. For more information, see "REST Services for Reporting" in the *Identity Reporting Module Guide*.

Data Collection Service Driver: A driver that captures changes to objects store in an Identity Vault, such as accounts, roles, resources, groups, and team memberships. The Data Collection Service driver registers itself with the Data Collection Service and pushes change events (such as data synchronization, add, modify, and delete events) to the Data Collection Service.

The information captured records changes to these objects:

- User accounts and identities
- Roles and role levels
- Groups

  NOTE: The reporting module does not support dynamic groups and only generates reports on static group data.

- Group memberships
- Provisioning Request Definitions
- Separation of Duties definitions and violations
- User entitlement associations
- Resource definitions and resource parameters

- Role and resource assignments
- Identity Vault entitlements, entitlement types, and drivers

Managed System Gateway Driver: A driver that collects information from managed systems. To retrieve the managed system data, the driver queries the Identity Vault. The data retrieved includes the following:

- List of all managed systems
- List of all accounts for the managed systems
- Entitlement types, values, and assignments, and user account profiles for the managed systems

Identity Reporting: The user interface for the reporting module makes it easy to schedule reports to run at off-peak times to optimize performance. For more information about the Identity Reporting Module, see the *Identity Reporting Module Guide*.

Reports: Identity Manager contains predefined reports to display the information in the Identity Information Warehouse in useful and consumable ways. You can also create custom reports. For more information about the reports, see *Using Identity Manager 4.0 Reports*. For information about custom reports, see "Creating Custom Report Definitions" in the *Identity Reporting Module Guide*.

Non-Managed Application REST End Point: A non-managed application is an application that is not connected to an Identity Vault, but nonetheless includes data that you want to report on. By defining a REST end point for an application, you make it possible for the reporting module to collect data from this application.

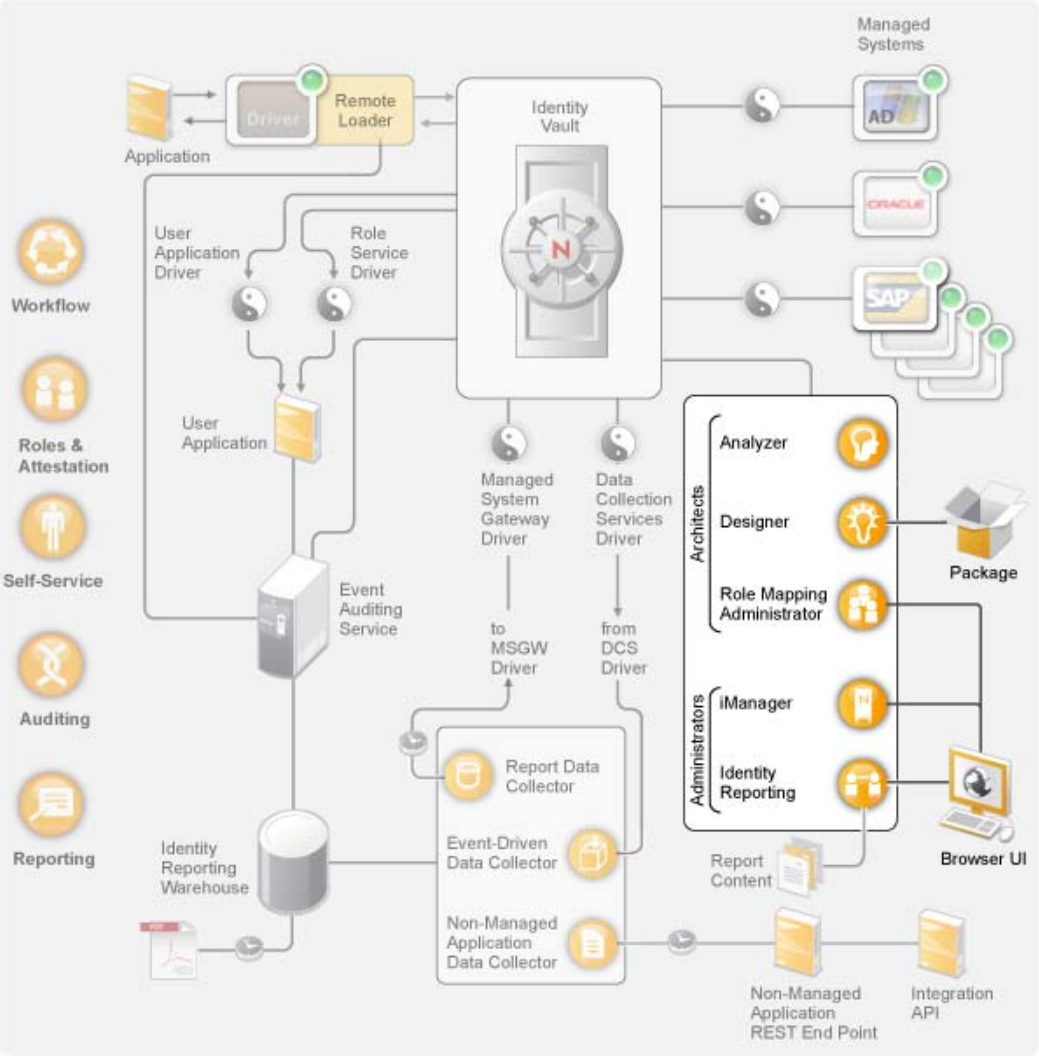
Integration API: The initial release of the Identity Reporting Module provides support for a single REST API. This API allows you to implement a REST end point for a non-managed application.

Identity Manager Tools

4

Identity Manager provides tools that help you create and maintain your Identity Manager solution. Each of the tools has a specific function.

Figure 4-1 *Identity Manager Tools*



You use Designer to design, create, and configure your Identity Manager system in an off-line environment and then deploy your changes to your live system. Designer also provides you the package management capabilities for pre-configuring and customizing Identity Manager driver policies. Analyzer is used when you create your Identity Manager solution to analyze, clean, and prepare you data for synchronization.

The Role Mapping Administrator is used to create and manage roles throughout your Identity Manager solution.

You can use iManager to perform the similar tasks as Designer and also monitor the health of your system; however, package management is not supported in iManager. We recommend that you use iManager for administration tasks and Designer for configuration tasks that require changes to packages, modeling, and testing prior to deployment.

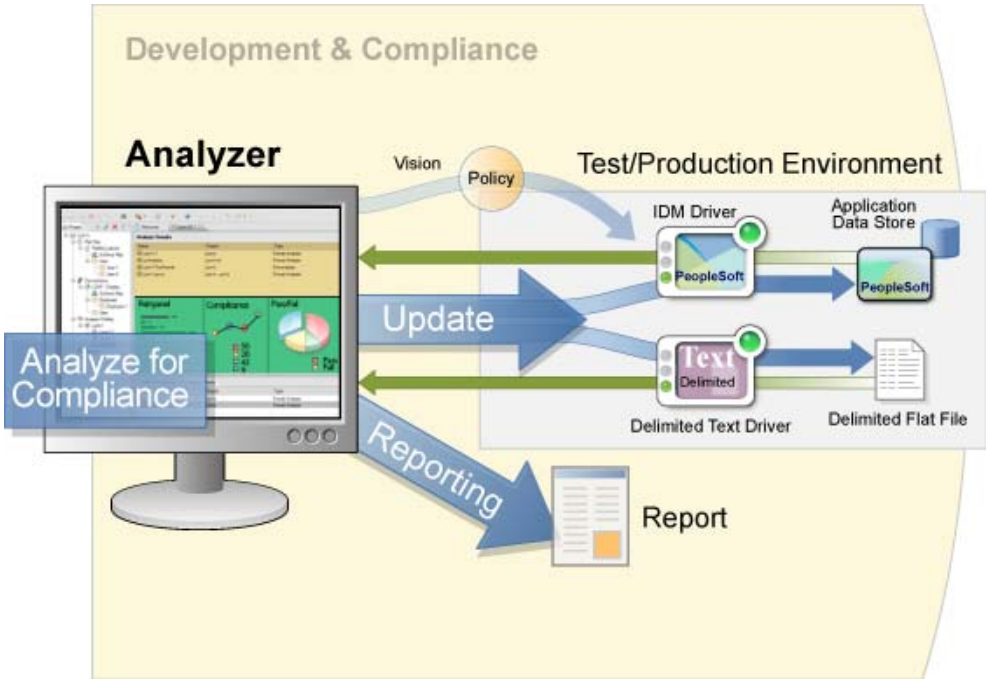
More information about each of these tools is provided in the following sections:

- Section 4.1, "Analyzer," on page 32
- Section 4.2, "Designer," on page 32
- Section 4.3, "iManager," on page 33
- Section 4.4, "Role Mapping Administrator," on page 34
- Section 4.5, "Identity Reporting," on page 35

4.1 Analyzer

Analyzer is an Eclipse-based identity management toolset that helps you ensure that internal data quality policies are adhered to by providing data analysis, data cleansing, data reconciliation, and data monitoring and reporting. Analyzer lets you analyze, enhance, and control all data stores throughout the enterprise.

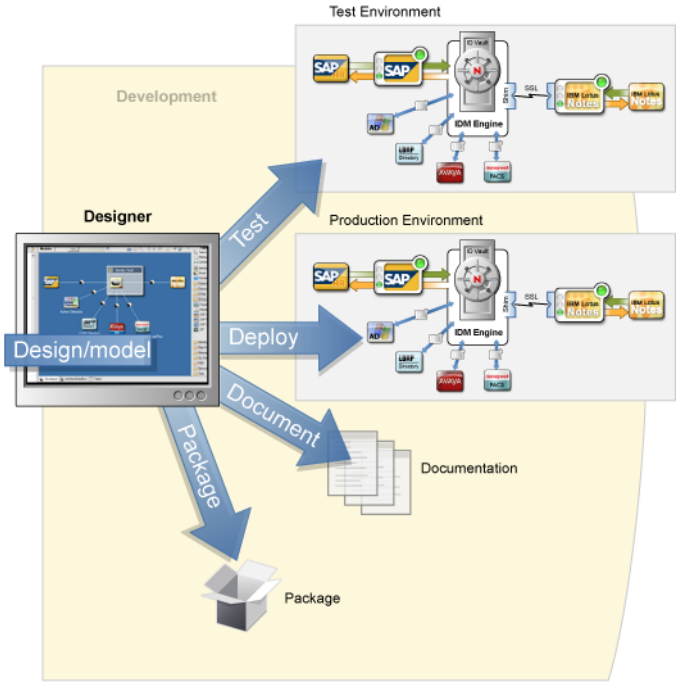
Figure 4-2 *Analyzer for Identity Manager*



4.2 Designer

Designer is an Eclipse-based tool that helps you design, deploy, and document your Identity Manager system. Using Designer's graphical interface, you can design and test your system in an offline environment, deploy the system into your production environment, and document all details of your deployed system.

Figure 4-3 *Designer for Identity Manager*



Design: Designer provides a graphical interface through which you can model your system. This includes views that allow you to create and control the connections between Identity Manager and applications, configure policies, and manipulate how data flows between connected applications.

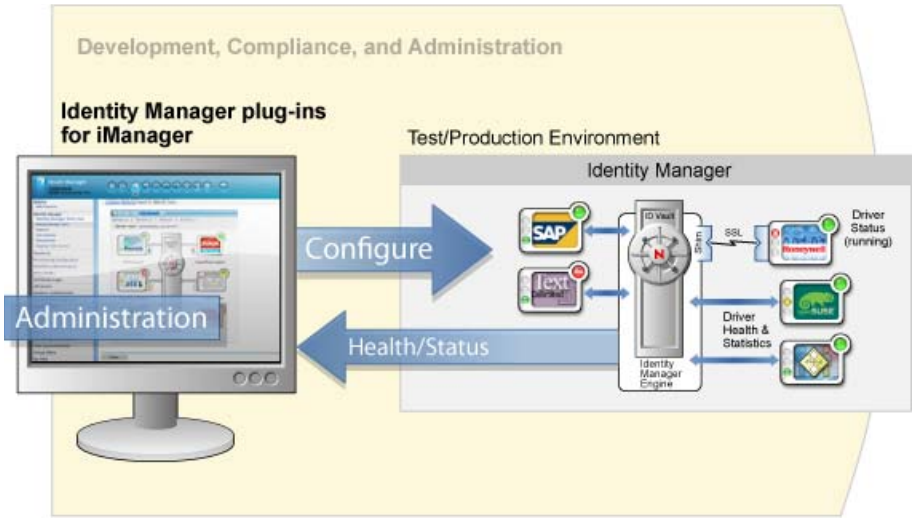
Deploy: The work you do in Designer is deployed to your production environment only when you initiate the deployment. This gives you the freedom to experiment, test the results, and resolve any issues before going live in your production environment.

Document: You can generate extensive documentation that shows your systems hierarchy, driver configurations, policy configurations, and much more. Basically, you have all the information needed to understand the technical aspects of your system while helping you verify compliance with your business rules and policies.

4.3 iManager

Novell iManager is a browser-based tool that provides a single point of administration for many Novell products, including Identity Manager. By using the Identity Manager plug-ins for iManager, you can manage Identity Manager and receive real-time health and status information about your Identity Manager system.

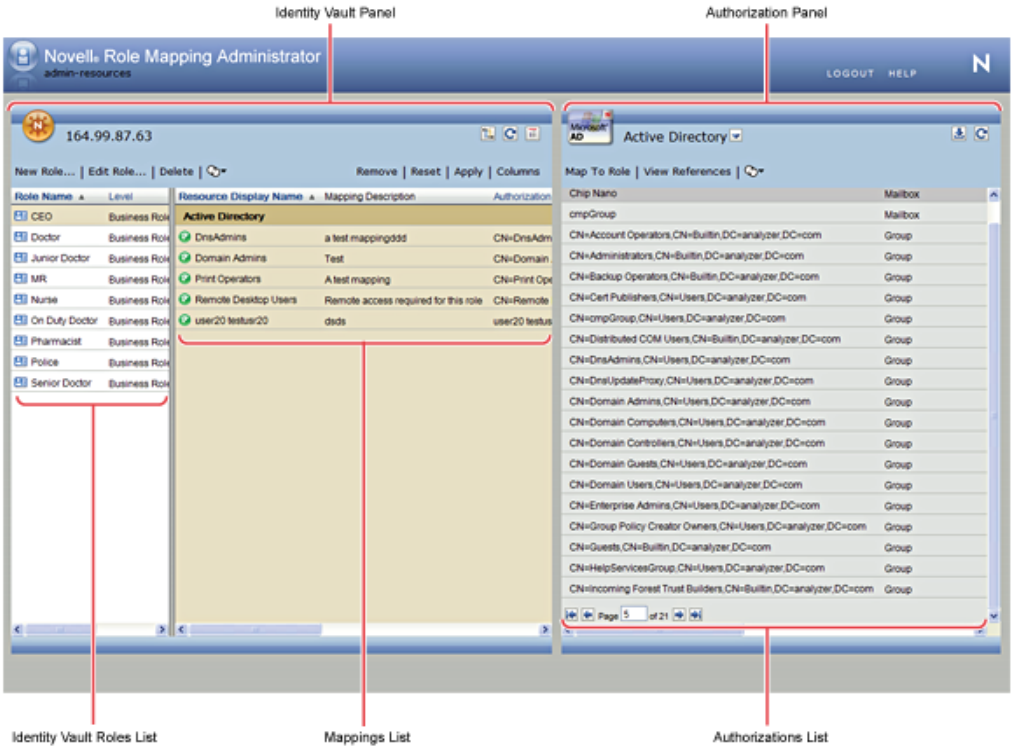
Figure 4-4 *Novell iManager*



4.4 Role Mapping Administrator

The Role Mapping Administrator is a Web service that discovers authorizations and permissions that can be granted within your major IT systems. It allows business analysts, not just IT administrators, to define and maintain which authorizations are associated with which business roles.

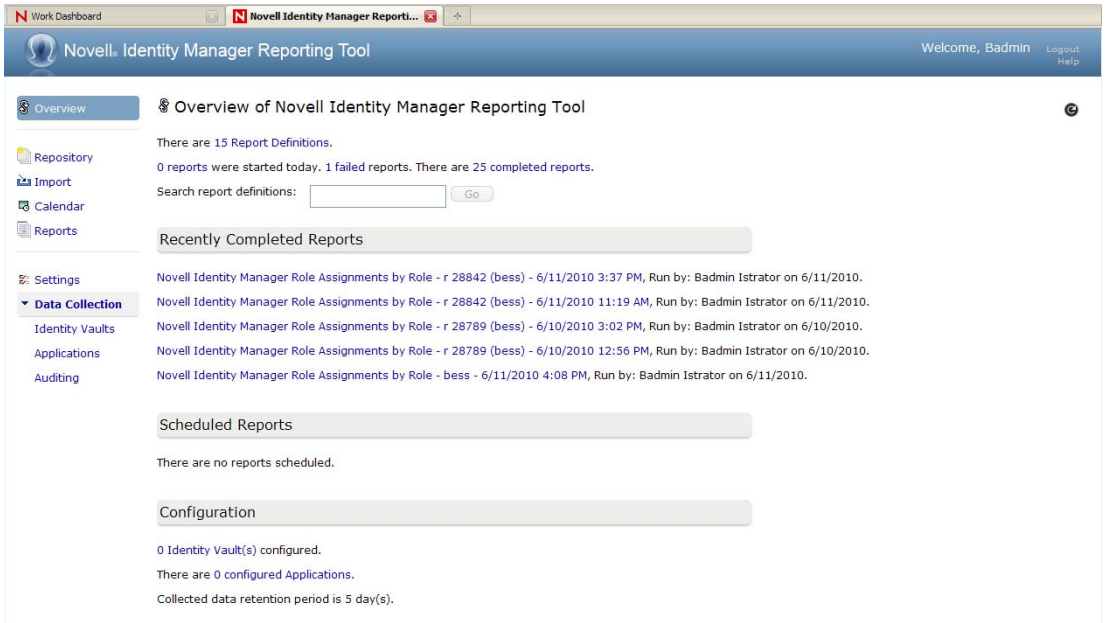
Figure 4-5 *Role Mapping Administrator*



4.5 Identity Reporting

The Identity Reporting Module generates reports that show critical business information about various aspects of your Identity Manager configuration, including information collected from Identity Vaults and managed systems such as Active Directory or SAP. The reporting module provides a set of predefined report definitions you can use to generate reports. In addition, it gives you the option to import custom reports defined in a third-party tool. The user interface for the reporting module makes it easy to schedule reports to run at off-peak times to optimize performance.

Figure 4-6 *Identity Reporting Module*



The reporting module provides several open integration points. For example, if you want to collect data about third-party applications that are not connected to Identity Manager, you can implement a custom REST endpoint to collect data from these applications. In addition, you can customize the data that is pushed to the Identity Vault. After this data is available, you can write custom reports to see this information.

What's Next

5

After you understand the components that make up Identity Manager 4.0, the next step is to use the documentation to create your Identity Manager solution. The following sections explain where to find the documentation for the tasks listed:

- Section 5.1, "Planning an Identity Manager Solution," on page 37
- Section 5.2, "Preparing Your Data for Synchronization," on page 37
- Section 5.3, "Installing or Upgrading Identity Manager," on page 37
- Section 5.4, "Configuring Identity Manager," on page 38
- Section 5.5, "Administering Identity Manager," on page 39

5.1 Planning an Identity Manager Solution

The first step in designing an Identity Manager solution is to decide exactly what you want your solution to do in your business. Use the "Planning" section in the *Identity Manager 4.0 Framework Installation Guide* to create a plan for your Identity Manager solution by using Designer. You can also design your User Application solution by using the *User Application: Design Guide*.

Designer allows you to capture information into a project and share the information with other people. You can also model the solution in Designer before you start making changes. For more information about Designer see *Understanding Designer for Identity Manager*.

5.2 Preparing Your Data for Synchronization

After you create your plan, you need to prepare the data in your environment for synchronization. Analyzer is the tool you use to analyze, clean, and prepare the data for synchronization. For more information, see the *Analyzer 1.2 for Identity Manager Administration Guide*.

5.3 Installing or Upgrading Identity Manager

When you have created your plan and prepared the data, you can install Identity Manager. If you have a small to medium IT environment and you haven't used Identity Manager before, it is best to use the integrated installer. The integrated installer installs and configures all components that come with Identity Manager. For more information, see the *Identity Manager 4.0 Integrated Installation Guide*.

If you have an existing Identity Manager system or you have a large IT environment, use the *Identity Manager 4.0 Framework Installation Guide* to install or upgrade the different Identity Manager components. Each Identity Manager manager component is installed and configured separately, so you can customize your Identity Manager solution.

- For installation instructions, see "Installation" in the *Identity Manager 4.0 Framework Installation Guide*.
- For upgrade instructions, see "Performing an Upgrade" in the *Identity Manager 4.0 Framework Installation Guide*.

- If you are migrating an existing system to new hardware, see "Performing a Migration" in the *Identity Manager 4.0 Framework Installation Guide*.
- If you need to migrate the Roles Based Provisioning Module, see the *Identity Manager Roles Based Provisioning Module 4.0 User Application: Migration Guide*.

5.4 Configuring Identity Manager

After Identity Manager is installed, you must configure different components to have a fully functioning solution.

- Section 5.4.1, "Synchronizing Data," on page 38
- Section 5.4.2, "Mapping Roles," on page 38
- Section 5.4.3, "Configuring the User Application," on page 38
- Section 5.4.4, "Configuring Auditing, Reporting, and Compliance," on page 39

5.4.1 Synchronizing Data

Identity Manager uses drivers to synchronize data between different applications, databases, operating systems, and directories. After Identity Manager is installed, you need to create and configure one or more drivers for each system you want to synchronize data with.

Each driver has a documentation guide that explains the requirements and configuration steps required to synchronize data. The driver guides are located at the Identity Manager 4.0 Drivers documentation Web site (http://www.novell.com/documentation/idm40drivers/index.html).

Use the specific driver guide for each managed system to create a driver to synchronize identity data.

5.4.2 Mapping Roles

When you have information synchronizing between the different systems, use the Role Mapping Administrator (RMA) to manage the roles in the different systems. For more information, see the *Novell Identity Manager Role Mapping Administrator 2.0 User Guide*.

5.4.3 Configuring the User Application

The next step is to add a business perspective to the Identity Manager solution with the User Application. The User Application enables you to address the following business needs:

- Providing a convenient way to perform roles-based provisioning actions.
- Ensuring that your organization has a method for verifying that personnel are fully aware of organizational policies and are taking steps to comply with these policies.
- Providing user self-service, allowing a new user to self-register, and providing access to anonymous or guest users.
- Ensuring that access to corporate resources complies with organizational policies and that provisioning occurs within the context of the corporate security policy.
- Reducing the administrative burden of entering, updating, and deleting user information across all systems in the enterprise.

- Managing manual and automated provisioning of identities, services, resources, and assets.
- Supporting complex workflows.

The *Identity Manager Roles Based Provisioning Module 4.0 User Application: Administration Guide* contains the information on how to configure these features of the User Application.

5.4.4 Configuring Auditing, Reporting, and Compliance

The last and most important step in creating your Identity Manager solution is to configure the auditing, reporting, and compliance features so you can verify that your solution is in compliance with your business policies. Use the following guides to set up and configure these features:

- **Auditing:** See the *Identity Manager 4.0 Reporting Guide for Novell Sentinel*.
- **Reporting:** See the *Identity Reporting Module Guide* and *Using Identity Manager 4.0 Reports*.
- **Compliance:** See "Using the Compliance Tab" in the *Identity Manager Roles Based Provisioning Module 4.0 User Application: User Guide*.

5.5 Administering Identity Manager

After your Identity Manager solution is complete, there are many different guides that help you administer, maintain, and change your Identity Manager solution as your business changes and grows. The different administration guides are located on the Identity Manager 4.0 documentation Web site (http://www.novell.com/documentation/idm40/index.html) under the Administration heading.