Überblick

Novell®
Identity Manager

3.6.1

15. Mai 2009

www.novell.com

Rechtliche Hinweise

Novell, Inc. übernimmt für Inhalt oder Verwendung dieser Dokumentation keine Haftung und schließt insbesondere jede ausdrückliche oder implizite Garantie für Marktfähigkeit oder Eignung für einen bestimmten Zweck aus. Novell, Inc. behält sich das Recht vor, dieses Dokument jederzeit teilweise oder vollständig zu ändern, ohne dass für Novell, Inc. die Verpflichtung entsteht, Personen oder Organisationen davon in Kenntnis zu setzen.

Novell, Inc. gibt ebenfalls keine Erklärungen oder Garantien in Bezug auf Novell-Software und schließt insbesondere jede ausdrückliche oder implizite Garantie für handelsübliche Qualität oder Eignung für einen bestimmten Zweck aus. Außerdem behält sich Novell, Inc. das Recht vor, Novell-Software jederzeit ganz oder teilweise zu ändern, ohne dass für Novell, Inc. die Verpflichtung entsteht, Personen oder Organisationen von diesen Änderungen in Kenntnis zu setzen.

Alle im Zusammenhang mit dieser Vereinbarung zur Verfügung gestellten Produkte oder technischen Informationen unterliegen möglicherweise den US-Gesetzen zur Exportkontrolle sowie den Handelsgesetzen anderer Länder. Sie stimmen zu, alle Gesetze zur Exportkontrolle einzuhalten und alle für den Export, Reexport oder Import von Lieferungen erforderlichen Lizenzen oder Klassifikationen zu erwerben. Sie erklären sich damit einverstanden, nicht an juristische Personen, die in der aktuellen US-Exportausschlussliste enthalten sind, oder an in den US-Exportgesetzen aufgeführte terroristische Länder oder Länder, die einem Embargo unterliegen, zu exportieren oder zu reexportieren. Sie stimmen zu, keine Lieferungen für verbotene nukleare oder chemisch-biologische Waffen oder Waffen im Zusammenhang mit Flugkörpern zu verwenden. Weitere Informationen zum Export von Novell-Software finden Sie auf der Website Novell International Trade Services (http://www.novell.com/company/policies/trade_services). Novell übernimmt keine Verantwortung für das Nichteinholen notwendiger Exportgenehmigungen.

Novell, Inc. besitzt Rechte auf geistiges Eigentum für die Technologie, die in dem in diesem Dokument beschriebenen Produkt integriert ist. Diese Rechte auf geistiges Eigentum umfassen möglicherweise insbesondere ein oder mehrere Patente in den USA, die auf der Webseite Novell Legal Patents (http://www.novell.com/company/legal/patents/) aufgeführt sind, sowie ein oder mehrere andere Patente oder laufende Patentanträge in den USA und in anderen Ländern.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
USA.
www.novell.com

Online-Dokumentation: Die neueste Online-Dokumentation für dieses und andere Novell-Produkte finden Sie auf der Dokumentations-Webseite von Novell (http://www.novell.com/documentation).

Novell-Marken

Hinweise zu Novell-Marken finden Sie in der Novell Trademark and Service Mark-Liste (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materialien von Drittanbietern

Die Rechte für alle Marken von Drittanbietern liegen bei den jeweiligen Eigentümern.

Inhalt

Informationen zu diesem Handbuch

In diesem Handbuch werden die geschäftsbezogenen Probleme vorgestellt, bei deren Lösung Novell® Identity Manager Ihnen behilflich sein kann. Ferner wird ein technischer Überblick über die Software-Komponenten und Werkzeuge von Identity Manager gegeben, die Sie mit Ihrer Software verwenden können. Dieses Handbuch gliedert sich wie folgt:

Zielgruppe

Dieses Handbuch ist für Administratoren, Berater und Netzwerktechniker gedacht, die eine detaillierte Einführung in die Geschäftslösungen, Technologien und Werkzeuge von Identity Manager benötigen.

Aktualisierungen für Dokumentationen

Die neueste Version dieses Dokuments finden Sie auf der Website zur Identity Manager-Dokumentation (http://www.novell.com/documentation/idm36/index.html).

Zusätzliche Dokumentation

Die Dokumentation für andere Identity Manager-Treiber finden Sie auf der Website für Identity Manager-Treiber (http://www.novell.com/documentation/idm36drivers/index.html).

Konventionen in der Dokumentation

In dieser Novell-Dokumentation wird ein „Größer als“-Zeichen (>) verwendet, um verschiedene Aktionen innerhalb eines Schritts und Meldungen in einem Querverweispfad voneinander zu trennen.

Ein Markensymbol (®, ™ usw.) kennzeichnet eine Novell-Marke. Ein Sternchen (*) kennzeichnet eine Drittanbieter-Marke.

Wenn ein Pfadname für bestimmte Plattformen mit einem umgekehrten Schrägstrich und für andere Plattformen mit einem Schrägstrich geschrieben werden kann, wird der Pfadname in diesem Handbuch mit einem umgekehrten Schrägstrich dargestellt. Benutzer von Plattformen, die einen Schrägstrich erfordern, wie z. B. Linux* oder UNIX*, sollten die für die Software erforderlichen Schrägstriche verwenden.

1 Automatisierung von Geschäftsprozessen mit Identity Manager

Nachfolgend werden einige der Geschäftsprozesse beschrieben, die Sie durch die Implementierung eines Novell® Identity Manager-Systems automatisieren können. Wenn Sie die Identity Manager-Lösungen zur Automatisierung von Geschäftsprozessen bereits kennen, können Sie direkt mit der technischen Einführung unter Kapitel 2, „Identity Manager-Architektur“, auf Seite 19 fortfahren.

Das Verwalten von Identitätsanforderungen stellt in den meisten Unternehmen eine Kernfunktion dar. Stellen Sie sich beispielsweise einmal vor, es ist früh an einem Montagmorgen. Sie gehen die Liste der Anforderungen in Ihrer Warteschlange durch:

- Die Handynummer von Joachim Schmidt hat sich geändert. Sie müssen sie in der Personaldatenbank und in vier weiteren unabhängigen Systemen aktualisieren.
- Karen Hansen, die gerade aus einem längeren Urlaub zurückgekehrt ist, hat ihr Email-Passwort vergessen. Sie müssen ihr helfen, es wiederzuerlangen oder zurückzusetzen.
- Hans Müller hat gerade einen neuen Mitarbeiter eingestellt. Sie müssen für den neuen Mitarbeiter den Netzwerkzugriff und ein Email-Konto einrichten.
- Ida Moser benötigt Zugriff auf die Oracle*-Finanzdatenbank, wofür Sie die Genehmigung von drei verschiedenen Vorgesetzten einholen müssen.
- Robert Meyer hat von der Buchhaltung in die Rechtsabteilung gewechselt. Sie müssen dafür sorgen, dass er Zugriff auf dieselben Ressourcen erhält wie die übrigen Mitarbeiter der Rechtsabteilung und dass sein Zugriff auf die Buchhaltungsressourcen gesperrt wird.
- Karl Jonas, Ihr eigener Chef, hat eine Kopie von Ida Mosers Bitte um Zugriff auf die Oracle-Finanzdatenbank erhalten und überlegt, ob nicht zu viele Mitarbeiter Zugriff darauf besitzen. Sie müssen für ihn einen Bericht erstellen, in dem alle Mitarbeiter mit Zugriff auf die Datenbank aufgeführt sind.

Sie atmen tief durch und beginnen mit der ersten Anforderung, wobei Ihnen bewusst ist, dass es schwierig wird, allen Anforderungen rechtzeitig nachzukommen, und dass Sie daneben kaum Zeit finden werden, Ihre anderen Projekte fertigzustellen.

Wenn dies für Sie oder Kollegen in Ihrem Unternehmen nach einem ganz normalen Arbeitstag klingt, ist Identity Manager die richtige Lösung für Sie. Die Kernfunktionen von Identity Manager, die auf der folgenden Abbildung vorgestellt werden, können Ihnen helfen, all diese Aufgaben und noch weitere zu automatisieren. Die Komponenten „Workflow“, „Rollen“, „Beglaubigung“, „Selbstbedienung“, „Revision“ und „Berichterstellung“, in deren Mittelpunkt die durch Ihre Geschäftsrichtlinien gesteuerte Datensynchronisierung zwischen mehreren Systemen steht, werden gemeinsam zur Automatisierung der Prozesse eingesetzt, die für die Bereitstellung für Benutzer und die Passwortverwaltung erforderlich sind – zwei der schwierigsten und zeitintensivsten Aufgaben einer IT-Organisation.

Abbildung 1-1 *Kernfunktionen von Identity Manager*

In den folgenden Abschnitten werden diese Funktionen von Identity Manager vorgestellt und es wird erläutert, wie sie Ihnen dabei helfen können, den Identitätsanforderungen Ihrer Organisation gerecht zu werden:

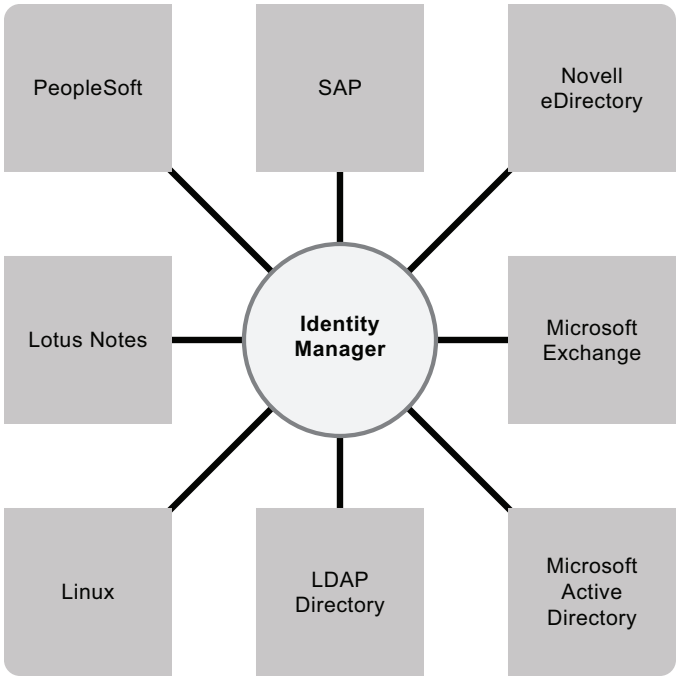
- Abschnitt 1.1, „Datensynchronisierung“, auf Seite 10
- Abschnitt 1.2, „Workflow“, auf Seite 13
- Abschnitt 1.3, „Rollen und Beglaubigung“, auf Seite 14
- Abschnitt 1.4, „Selbstbedienung“, auf Seite 15
- Abschnitt 1.5, „Revision und Berichterstellung“, auf Seite 17

1.1 Datensynchronisierung

In den meisten Organisationen sind Identitätsdaten in verschiedenen Systemen gespeichert. Möglicherweise sind bei Ihnen Identitätsdaten aber nur in einem System gespeichert, und Sie benötigen sie auch in einem anderen System. In beiden Fällen ist es erforderlich, dass Sie Daten schnell zwischen verschiedenen Systemen übertragen und synchronisieren können.

Mit Identity Manager können Sie Informationen über einen großen Umfang an Anwendungen, Datenbanken, Betriebssystemen und Verzeichnissen hinweg synchronisieren, transformieren und verteilen, z. B. Daten aus SAP*, PeopleSoft*, Lotus Notes*, Microsoft* Exchange, Microsoft Active Directory*, Novell eDirectory™, Linux und UNIX sowie LDAP-Verzeichnissen.

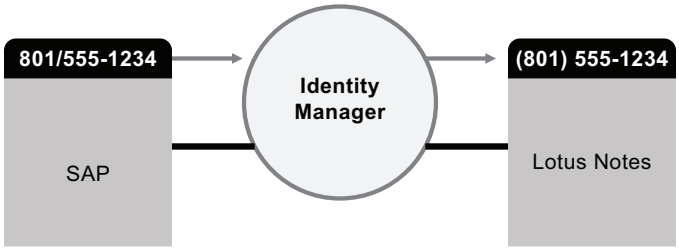
Abbildung 1-2 *Verbinden mehrerer Systeme mit Identity Manager*



Sie steuern den Datenfluss zwischen den verbundenen Systemen. Unter anderem bestimmen Sie, welche Daten gemeinsam genutzt werden, welches System die autorisierte Quelle für bestimmte Daten ist und wie die Daten interpretiert und transformiert werden, um den Anforderungen anderer Systeme gerecht zu werden.

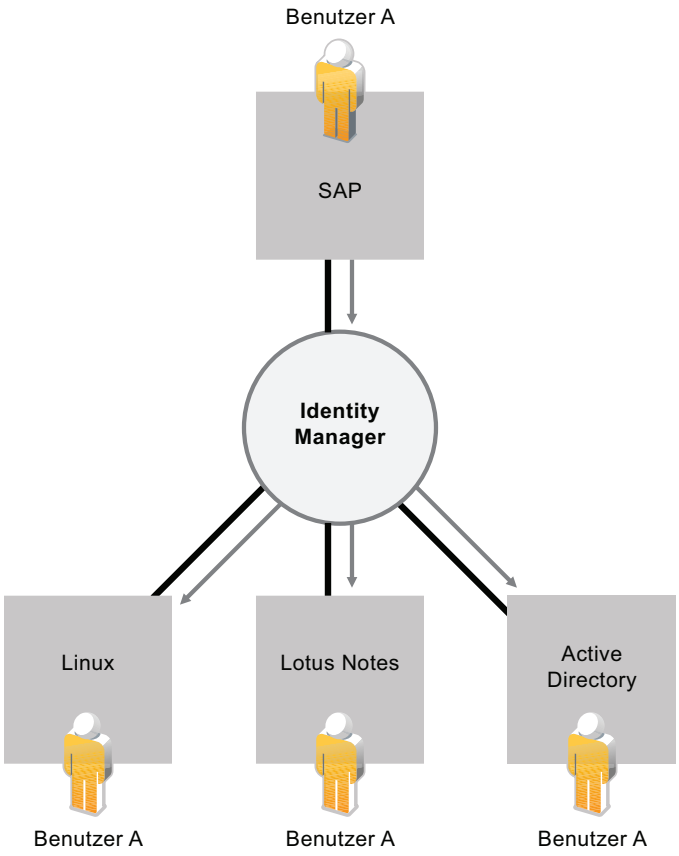
Im nachfolgenden Diagramm ist die SAP-Personaldatenbank die autorisierte Quelle für die Telefonnummer eines Benutzers. Das Lotus Notes-System verwendet ebenfalls Telefonnummern, daher wandelt Identity Manager die Nummer in das erforderliche Format um und überträgt sie an das Lotus Notes-System. Jedes Mal, wenn die Telefonnummer im SAP-Personalsystem geändert wird, werden die Daten im Lotus Notes-System synchronisiert.

Abbildung 1-3 *Datensynchronisierung verbundener Systeme*



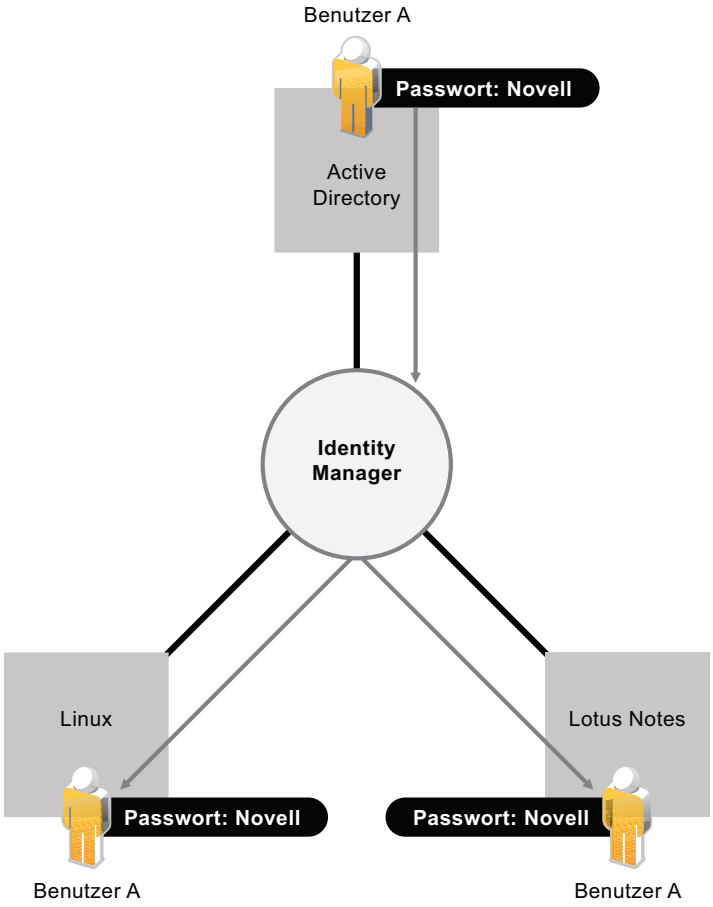
Das Verwalten der Daten vorhandener Benutzer stellt nur die erste Ebene der Datensynchronisierungsfunktionen von Identity Manager dar. Zusätzlich können mit Identity Manager in Verzeichnissen wie Active Directory, auf Systemen wie PeopleSoft und Lotus Notes und unter Betriebssystemen wie UNIX und Linux neue Benutzerkonten erstellt und vorhandene Konten entfernt werden. Wenn Sie beispielsweise einen neuen Mitarbeiter zu Ihrem SAP-Personalsystem hinzufügen, kann Identity Manager automatisch ein neues Benutzerkonto in Active Directory, ein neues Konto in Lotus Notes und ein neues Konto in einem Linux NIS-Kontenverwaltungssystem erstellen.

Abbildung 1-4 *Erstellung von Benutzerkonten in verbundenen Systemen*



Im Rahmen der Datensynchronisierungsfunktion kann Identity Manager Sie auch bei der Synchronisierung von Passwörtern zwischen verschiedenen Systemen unterstützen. Wenn ein Benutzer beispielsweise sein Passwort in Active Directory ändert, kann Identity Manager diese Änderung an Lotus Notes und Linux weitergeben.

Abbildung 1-5 *Passwortsynchronisierung verbundener Systeme*

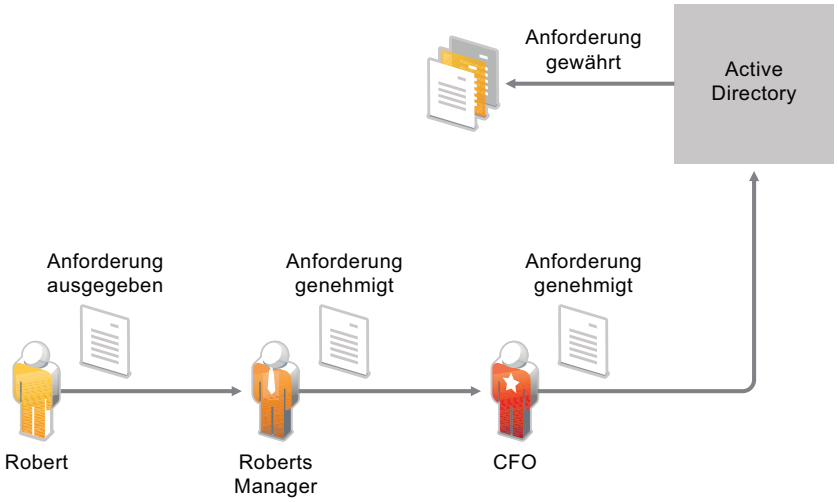


1.2 Workflow

Wahrscheinlich ist für den Zugriff auf viele Ressourcen in Ihrer Organisation keine Genehmigung erforderlich. Möglicherweise ist der Zugriff auf einige Ressourcen jedoch beschränkt und muss von einer oder mehreren Personen genehmigt werden.

Identity Manager bietet Workflow-Funktionen, die sicherstellen, dass bei Ihren Bereitstellungsprozessen die richtigen Ressourcen-Genehmiger einbezogen werden. Nehmen Sie beispielsweise an, dass Robert, für den bereits ein Active Directory-Konto eingerichtet wurde, über Active Directory auf Finanzberichte zugreifen muss. Dies muss von Roberts unmittelbarem Vorgesetzten sowie vom Leiter der Finanzabteilung genehmigt werden. Hierzu können Sie einen Genehmigungsworkflow einrichten, der Roberts Anforderung zunächst an seinen Vorgesetzten und sobald dieser die Genehmigung erteilt hat an den Leiter der Finanzabteilung weiterleitet. Wenn der Leiter der Finanzabteilung seine Genehmigung erteilt hat, wird die automatische Bereitstellung der von Robert zum Zugriff und zur Ansicht der Finanzdokumente benötigten Active Directory-Rechte veranlasst.

Abbildung 1-6 *Genehmigungsworkflow für die Bereitstellung für Benutzer*



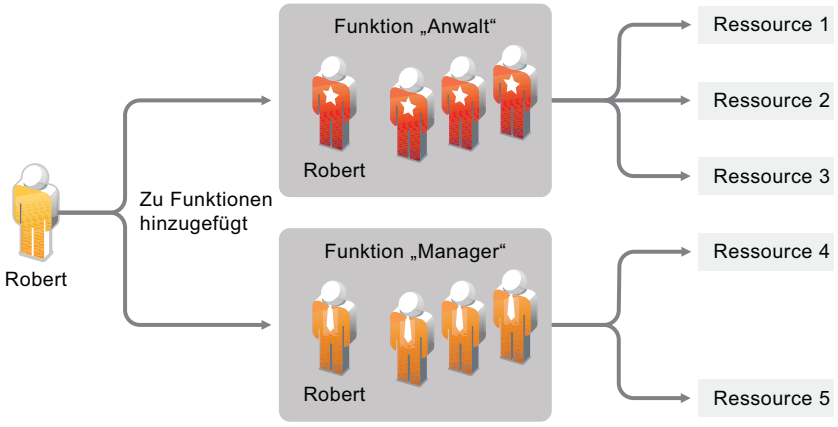
Workflows können automatisch initiiert werden, sobald ein bestimmtes Ereignis eintritt (z. B. wenn ein neuer Benutzer zu Ihrem Personalsystem hinzugefügt wird), oder sie können manuell durch eine Benutzeranforderung initiiert werden. Sie können sicherstellen, dass Genehmigungen rechtzeitig erteilt werden, indem Sie Vertretungsgenehmiger und Genehmigungsteams einrichten.

1.3 Rollen und Beglaubigung

Oft hängt es von der Rolle eines Mitarbeiters in einer Organisation ab, auf welche Ressourcen er Zugriff benötigt. Zum Beispiel benötigen die Anwälte einer Kanzlei vermutlich auf andere Ressourcen Zugriff als die Anwaltsgehilfen.

Mit Identity Manager können Sie die Bereitstellung für Benutzer abhängig von deren Rolle innerhalb der Organisation durchführen. Definieren Sie Rollen und nehmen Sie Zuweisungen entsprechend den Anforderungen Ihrer Organisation vor. Wenn einem Benutzer eine Rolle zugewiesen wird, stellt Identity Manager für den Benutzer den Zugriff auf die Ressourcen bereit, die der Rolle zugeordnet sind. Wenn einem Benutzer mehrere Rollen zugewiesen werden, erhält er Zugriff auf alle Ressourcen, die diesen Rollen zugewiesen sind, wie in der folgenden Abbildung dargestellt ist.

Abbildung 1-7 *Rollenbasierte Bereitstellung von Ressourcen*



Sie können festlegen, dass Benutzer automatisch Rollen hinzugefügt werden, wenn in Ihrer Organisation ein bestimmtes Ereignis eintritt (z. B. wenn ein neuer Benutzer mit der Stellenbezeichnung „Anwalt“ zu Ihrer SAP-Personaldatenbank hinzugefügt wird). Wenn für das Hinzufügen eines Benutzers zu einer Rolle eine Genehmigung erforderlich ist, können Sie Workflows einrichten, mit deren Hilfe Rollenanforderungen an die entsprechenden Genehmiger weitergeleitet werden. Sie können Benutzer auch manuell zu Rollen hinzufügen.

Es kann vorkommen, dass bestimmte Rollen nicht derselben Person zugewiesen werden dürfen, da die Rollen im Widerspruch zueinander stehen. Identity Manager bietet die Möglichkeit zur Funktionstrennung, mit deren Hilfe Sie verhindern können, dass Benutzern widersprüchliche Rollen zugewiesen werden, sofern nicht ein Mitarbeiter Ihrer Organisation eine Ausnahme für den Konflikt macht.

Da Rollenzuweisungen den Zugriff der Benutzer auf die Ressourcen Ihrer Organisation festlegen, ist es äußerst wichtig, die Korrektheit der Zuweisungen sicherzustellen. Falsche Zuweisungen können die Einhaltung von Unternehmens- und behördlichen Bestimmungen gefährden. Mit Identity Manager können Sie die Richtigkeit der Rollenzuweisungen durch einen Beglaubigungsprozess validieren. Mithilfe dieses Prozesses zertifizieren die verantwortlichen Mitarbeiter innerhalb Ihrer Organisation die den Rollen zugewiesenen Daten:

- **Benutzerprofilbeglaubigung:** Ausgewählte Benutzer bestätigen ihre eigenen Profilinformationen (Vorname, Nachname, Stellenbezeichnung, Abteilung, Email-Adresse usw.) und korrigieren falsche Angaben. Die Richtigkeit der Profilinformationen ist für korrekte Rollenzuweisungen ausschlaggebend.
- **Funktionstrennungsverletzungsbeglaubigung:** Verantwortliche Mitarbeiter prüfen einen Funktionstrennungsverletzungsbericht und bestätigen die Richtigkeit des Berichts. In dem Bericht sind alle Ausnahmen aufgeführt, die es erlauben, einem Benutzer widersprüchliche Rollen zuzuweisen.
- **Rollenzuweisungsbeglaubigung:** Verantwortliche Mitarbeiter prüfen einen Bericht, in dem ausgewählte Rollen zusammen mit den Benutzern, Gruppen und Rollen aufgeführt sind, die den einzelnen Rollen zugewiesen sind. Die verantwortlichen Mitarbeiter müssen dann die Korrektheit der Informationen bestätigen.
- **Benutzerzuweisungsbeglaubigung:** Verantwortliche Mitarbeiter prüfen einen Bericht, in dem ausgewählte Benutzer zusammen mit den Rollen aufgeführt sind, denen sie zugewiesen sind. Die verantwortlichen Mitarbeiter müssen dann die Korrektheit der Informationen bestätigen.

Diese Beglaubigungsberichte sollen Ihnen in erster Linie dabei helfen, sicherzustellen, dass die Rollenzuweisungen korrekt sind und dass es gültige Gründe für das Zulassen von Ausnahmen für widersprüchliche Rollen gibt.

1.4 Selbstbedienung

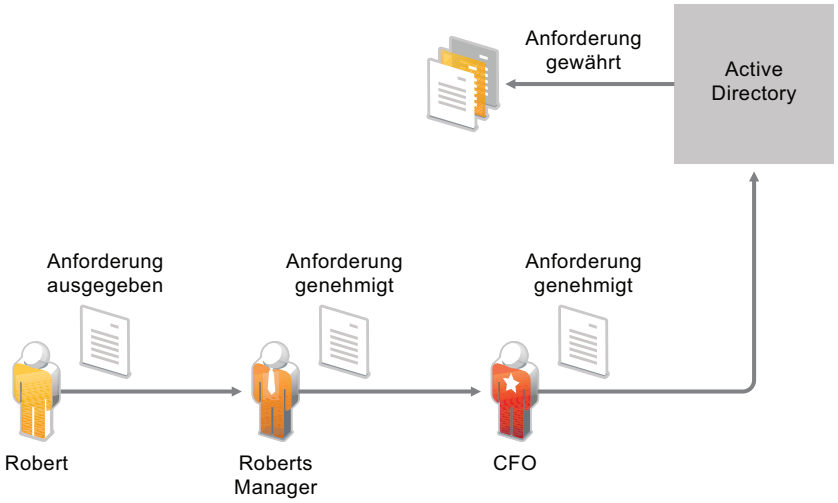
Vermutlich gibt es bei Ihnen Vorgesetzte und Abteilungen, die ihre Benutzerinformationen und Zugriffsanforderungen lieber selbst verwalten würden, als dies Ihnen oder Ihren Mitarbeitern zu überlassen. Wie oft haben Sie schon Sätze gehört wie, „Warum kann ich meine Handynummer in unserem Unternehmensverzeichnis nicht selbst ändern?“ Oder: „Ich arbeite in der Marketing-Abteilung. Warum muss ich den Helpdesk anrufen, um Zugriff auf die Marketing-Informationsdatenbank zu erhalten?“

Mit Identity Manager können Sie administrative Aufgaben an die Mitarbeiter delegieren, die dafür zuständig sein sollten. Zum Beispiel können Sie einzelnen Benutzern Folgendes ermöglichen:

- Das Verwalten ihrer persönlichen Daten im Unternehmensverzeichnis. Statt sich an Sie zu wenden, um eine Handynummer ändern zu lassen, können die Benutzer diese an einer Stelle ändern und die Änderung an alle Systeme weitergeben, die Sie über Identity Manager synchronisiert haben.
- Das Ändern ihrer Passwörter, das Einrichten eines Tipps für vergessene Passwörter sowie das Einrichten von Sicherheitsabfragen und -antworten für vergessene Passwörter. Statt Sie zu bitten, ein vergessenes Passwort zurückzusetzen, können die Benutzer dies selbst tun, nachdem sie einen Tipp erhalten oder eine Sicherheitsabfrage beantwortet haben.
- Das Anfordern von Zugriff auf Ressourcen wie Datenbanken, Systeme und Verzeichnisse. Die Benutzer müssen sich nicht mehr an Sie wenden, um den Zugriff auf eine Anwendung zu erhalten, sondern sie können die entsprechende Anwendung aus einer Liste von verfügbaren Ressourcen auswählen.

Zusätzlich zur Selbstbedienung für einzelne Benutzer bietet Identity Manager eine Selbstbedienungsverwaltung für Funktionen (Verwaltung, Helpdesk usw.) an, die für die Unterstützung, die Überwachung und die Genehmigung von Benutzeranforderungen verantwortlich sind. Betrachten Sie beispielsweise das unter Abschnitt 1.2, „Workflow“, auf Seite 13 verwendete und nachfolgend dargestellte Szenario.

Abbildung 1-8 *Bereitstellungs-Workflow mit Selbstbedienung*



Die Selbstbedienungsfunktion von Identity Manager wird nicht nur von Robert dazu verwendet, Zugriff auf die benötigten Dokumente anzufordern, sondern auch sein Vorgesetzter und der Leiter der Finanzabteilung verwenden sie für die Genehmigung der Anforderung. Der eingerichtete Genehmigungsworkflow ermöglicht Robert, seine Anforderung zu initiieren und ihren Fortschritt zu überwachen, und Roberts Vorgesetztem und dem Leiter der Finanzabteilung, auf seine Anforderung zu antworten. Wenn die Anforderung von Roberts Vorgesetztem und dem Leiter der Finanzabteilung genehmigt wird, veranlasst dies die Bereitstellung der von Robert zum Zugriff und zur Ansicht der Finanzdokumente benötigten Active Directory-Rechte.

1.5 Revision und Berichterstellung

Ohne Identity Manager kann die Bereitstellung für Benutzer ein mühsamer, zeitaufwändiger und kostenintensiver Vorgang sein. Einen noch bedeutend größeren Aufwand bringt es allerdings mit sich, zu überprüfen, ob die Bereitstellungsaktivitäten gemäß den Richtlinien, Anforderungen und Bestimmungen Ihrer Organisation erfolgen. Haben die richtigen Mitarbeiter Zugriff auf die richtigen Ressourcen? Haben die falschen Mitarbeiter keinen Zugriff auf dieselben Ressourcen? Hat der neue Mitarbeiter Zugriff auf das Netzwerk, seine Emails und die sechs weiteren für seine Arbeit erforderlichen Systeme? Wurde der Zugriff für den Mitarbeiter, der die Firma letzte Woche verlassen hat, gesperrt?

Mit Identity Manager haben Sie die Gewissheit, dass alle Benutzerbereitstellungsaktivitäten verfolgt und zu Revisionszwecken protokolliert werden. Identity Manager gibt für alle erfolgten Aktivitäten Ereignismeldungen aus. Mit Novell Sentinel™ können Sie diese Meldungen sammeln und daraus die folgenden Berichtarten generieren:

- Alle Genehmigungsworkflows in einem bestimmten Zeitraum, wobei die Aktionen („Gestartet“, „Weitergeleitet“, „Verweigert“, „Genehmigt“ usw.) für jeden Workflow aufgezeichnet werden.
- Alle in einem bestimmten Zeitraum bereitgestellten Ressourcen, wobei die Aktionen („Gesendet“, „Gewährt“, „Widerrufen“, „Ordnungsgemäß durchgeführt“ usw.) für jede Ressource aufgezeichnet werden.
- Alle Workflow-Statusangaben, Passwortänderungen und administrative Änderungen für einen Benutzer in einem bestimmten Zeitraum.
- Die gesamte Ressourcenbereitstellung für einen Benutzer in einem bestimmten Zeitraum.
- Die gesamte Ressourcenbereitstellung für alle Benutzer in einem bestimmten Zeitraum.

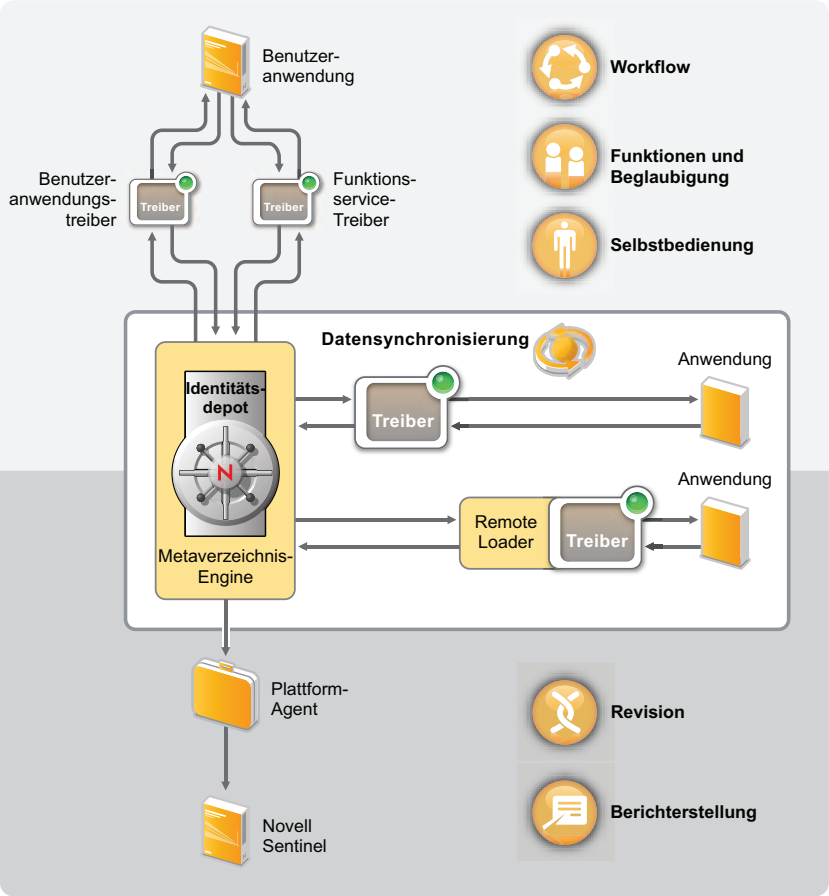
Novell Sentinel ist separat erhältlich.

Identity Manager-Architektur

2

Das folgende Diagramm zeigt die High-Level-Architekturkomponenten für die Novell® Identity Manager-Funktionen, die unter Kapitel 1, „Automatisierung von Geschäftsprozessen mit Identity Manager“, auf Seite 9 vorgestellt wurden: Datensynchronisierung, Workflow, Rollen, Beglaubigung, Selbstbedienung und Revision/Berichterstellung.

Abbildung 2-1 *High-Level-Architektur von Identity Manager*



Die einzelnen Komponenten werden in den folgenden Abschnitten erläutert:

- Abschnitt 2.1, „Datensynchronisierung“, auf Seite 19
- Abschnitt 2.2, „Workflow, Rollen, Beglaubigung und Selbstbedienung“, auf Seite 24
- Abschnitt 2.3, „Revision und Berichterstellung“, auf Seite 27

2.1 Datensynchronisierung

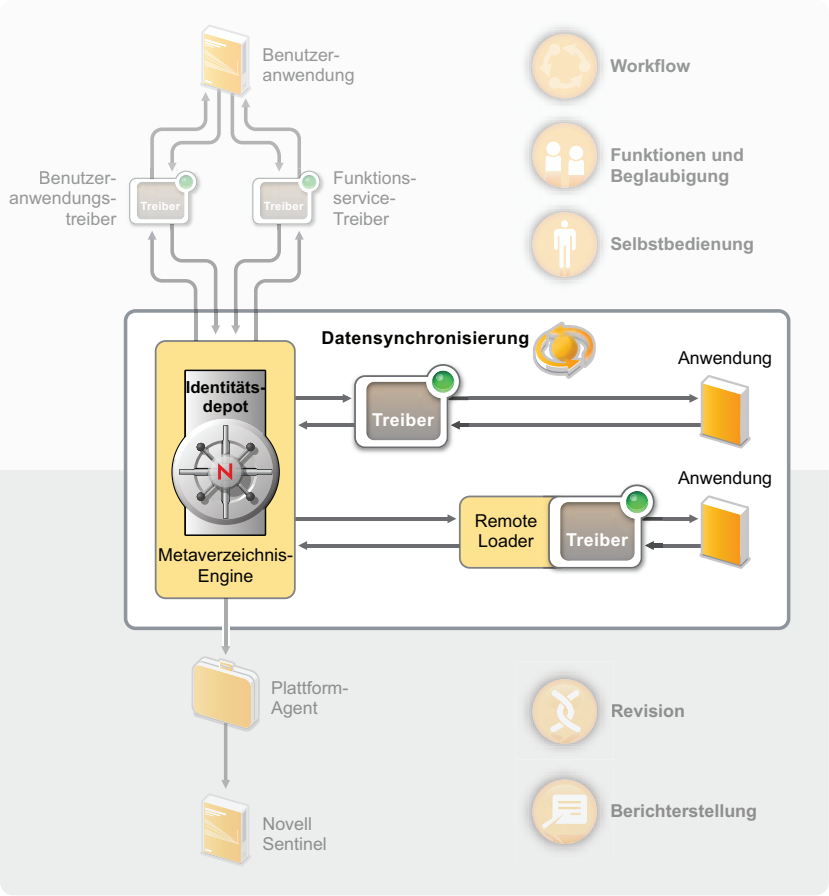
Die Datensynchronisierung bildet die Grundlage für die Automatisierung von Geschäftsprozessen. In ihrer einfachsten Form ist die Datensynchronisierung die Weitergabe von Daten von dem Speicherort, an dem ein Datenelement geändert wird, an andere Speicherorte, an denen es benötigt

wird. Wenn beispielsweise die Telefonnummer eines Mitarbeiters im Personalsystem einer Firma geändert wird, wird die Änderung idealerweise automatisch in allen anderen Systemen übernommen, in denen die Telefonnummer gespeichert ist.

Die Funktionen von Identity Manager gehen über die Synchronisierung von Identitätsdaten hinaus. Identity Manager kann alle Arten von Daten synchronisieren, die in der verbundenen Anwendung oder im Identitätsdepot gespeichert sind.

Die Datensynchronisierung wird einschließlich der Passwortsynchronisierung durch die fünf Basiskomponenten der Identity Manager-Lösung ermöglicht: das Identitätsdepot, die Metaverzeichnis-Engine, die Treiber, der Remote Loader und die verbundenen Anwendungen. Diese Komponenten sind im folgenden Diagramm abgebildet.

Abbildung 2-2 *Identity Manager-Architekturkomponenten*



In den folgenden Abschnitten finden Sie Beschreibungen dieser Komponenten und Erläuterungen der Konzepte, die Sie verstehen sollten, um in Ihrer Organisation eine erfolgreiche Datensynchronisierung zwischen verschiedenen Systemen durchführen zu können:

- Abschnitt 2.1.1, „Komponenten“, auf Seite 21
- Abschnitt 2.1.2, „Wichtige Konzepte“, auf Seite 21

2.1.1 Komponenten

Identitätsdepot: Das Identitätsdepot dient als Metaverzeichnis der Daten, die zwischen Anwendungen synchronisiert werden sollen. Zum Beispiel werden Daten, die von einem PeopleSoft-System nach Lotus Notes synchronisiert werden, zuerst zum Identitätsdepot hinzugefügt, bevor sie an das Lotus Notes-System gesendet werden. Außerdem werden im Identitätsdepot Identity Manager-spezifische Informationen gespeichert, z. B. Treiberkonfigurationen, Parameter und Richtlinien. Für das Identitätsdepot wird Novell eDirectory™ verwendet.

Metaverzeichnis-Engine: Wenn im Identitätsdepot oder in einer verbundenen Anwendung Daten geändert werden, verarbeitet die Metaverzeichnis-Engine die Änderungen. Bei Ereignissen, die im Identitätsdepot auftreten, verarbeitet die Engine die Änderungen und sendet über den Treiber Befehle an die Anwendung. Bei Ereignissen, die in der Anwendung auftreten, empfängt die Engine die Änderungen vom Treiber, verarbeitet diese und sendet Befehle an das Identitätsdepot. Die Metaverzeichnis-Engine wird auch als *Identity Manager-Engine* bezeichnet.

Treiber: Treiber stellen eine Verbindung zu den Anwendungen her, deren Identitätsinformationen Sie verwalten möchten. Ein Treiber hat zwei grundlegene Aufgaben: 1) das Melden von Datenänderungen (Ereignissen) in der Anwendung an die Metaverzeichnis-Engine sowie 2) das Ausführen von Datenänderungen (Befehlen), die von der Metaverzeichnis-Engine an die Anwendung gesendet werden.

Remote Loader: Die Treiber müssen auf demselben Server installiert und ausgeführt werden wie die Anwendung, zu der sie eine Verbindung herstellen. Wenn sich die Anwendung auf demselben Server wie die Metaverzeichnis-Engine befindet, müssen Sie lediglich den Treiber auf diesem Server installieren. Befindet sich die Anwendung jedoch nicht auf demselben Server wie die Metaverzeichnis-Engine (d. h. sie ist bezogen auf den Engine-Server remote, nicht lokal), müssen Sie den Treiber und den Remote Loader auf dem Server der Anwendung installieren. Der Remote Loader lädt den Treiber und kommuniziert an dessen Stelle mit der Metaverzeichnis-Engine.

Anwendung: Ein System, ein Verzeichnis, eine Datenbank oder ein Betriebssystem, zu dem der Treiber eine Verbindung herstellt. Die Anwendung muss APIs enthalten, die ein Treiber zum Ermitteln und Ausführen von Anwendungsdatenänderungen verwenden kann. Anwendungen werden häufig als *verbundene Systeme* bezeichnet.

2.1.2 Wichtige Konzepte

Kanäle: Der Datenfluss zwischen dem Identitätsdepot und einem verbundenen System erfolgt durch zwei separate *Kanäle*. Der *Abonnentenkanal* ermöglicht den Datenfluss vom Identitätsdepot zu einem verbundenen System. Anders ausgedrückt, das verbundene System abonniert Daten aus dem Identitätsdepot. Der *Herausgeberkanal* ermöglicht den Datenfluss von einem verbundenen System zum Identitätsdepot. Anders ausgedrückt, das verbundene System veröffentlicht Daten im Identitätsdepot.

Darstellung von Daten: Daten fließen als *XML-Dokumente* durch einen Kanal. Ein XML-Dokument wird erstellt, wenn eine Änderung im Identitätsdepot oder im verbundenen System auftritt. Das XML-Dokument wird an die Metaverzeichnis-Engine übergeben, die es mit den Filtern und Richtlinien verarbeitet, die dem Kanal des Treibers zugewiesen sind. Nachdem das XML-Dokument vollständig verarbeitet wurde, initiiert die Metaverzeichnis-Engine mithilfe des Dokuments die entsprechenden Änderungen im Identitätsdepot (Herausgeberkanal) bzw. der Treiber initiiert die entsprechenden Änderungen im verbundenen System (Abonnentenkanal).

Datenmanipulation: Wenn ein XML-Dokument durch einen Treiberkanal fließt, wirken sich die dem Kanal zugewiesenen *Richtlinien* auf die Dokumentdaten aus.

Richtlinien werden für viele Zwecke eingesetzt, z. B. zum Ändern von Datenformaten, zum Zuordnen von Attributen zwischen dem Identitätsdepot und dem verbundenen System, zum bedingungsabhängigen Blockieren des Datenflusses, zum Generieren von Email-Benachrichtigungen und zum Bearbeiten des Datenänderungstyps.

Steuerung des Datenflusses: *Filter* bzw. *Filterrichtlinien* steuern den Datenfluss. Filter geben an, welche Datenelemente zwischen dem Identitätsdepot und einem verbundenen System synchronisiert werden. Zum Beispiel werden Benutzerdaten in der Regel zwischen Systemen synchronisiert. Deshalb sind die Benutzerdaten bei den meisten verbundenen Systemen im Filter aufgelistet. Drucker hingegen sind üblicherweise für die meisten Anwendungen nicht von Interesse, daher sind Druckerdaten bei den meisten verbundenen Systemen nicht im Filter aufgeführt.

Bei jeder Beziehung zwischen dem Identitätsdepot und einem verbundenen System sind zwei Filter vorhanden: ein Filter im Abonnentenkanal, der den Datenfluss vom Identitätsdepot zum verbundenen System steuert, und ein Filter im Herausgeberkanal, der den Datenfluss vom verbundenen System zum Identitätsdepot steuert.

Autorisierte Quellen: Die meisten identitätsbezogenen Datenelemente haben einen konzeptionellen Eigentümer. Der Eigentümer eines Datenelements wird als *autorisierte Quelle* für das Element angesehen. In der Regel darf nur die autorisierte Quelle eines Datenelements Änderungen an dem Datenelement vornehmen.

Zum Beispiel wird das Email-System eines Unternehmens im Allgemeinen als autorisierte Quelle für die Email-Adresse eines Mitarbeiters betrachtet. Wenn ein Administrator des White Pages-Verzeichnis des Unternehmens die Email-Adresse eines Mitarbeiters in diesem System ändert, hat die Änderung keine Auswirkung darauf, ob der Mitarbeiter tatsächlich an die geänderte Adresse gesendete Emails empfängt, da die Änderung im Email-System erfolgen muss, damit sie wirksam ist.

Identity Manager legt autorisierte Quellen für ein Element mithilfe von Filtern fest. Wenn beispielsweise der Filter für die Beziehung zwischen dem PBX-System und dem Identitätsdepot zulässt, dass die Telefonnummer eines Mitarbeiters vom PBX-System in das Identitätsdepot, jedoch nicht vom Identitätsdepot zum PBX-System fließt, ist das PBX-System die autorisierte Quelle für die Telefonnummer. Wenn alle anderen Beziehungen verbundener Systeme zulassen, dass die Telefonnummer vom Identitätsdepot zu den verbundenen Systemen fließt, jedoch nicht in die umgekehrte Richtung, bedeutet dies, dass das PBX-System die einzige autorisierte Quelle für Telefonnummern von Mitarbeitern im Unternehmen ist.

Automatisierte Bereitstellung: Automatisierte Bereitstellung bedeutet, dass Identity Manager neben der reinen Synchronisierung von Datenelementen auch andere Benutzerbereitstellungsaktionen generieren kann.

Zum Beispiel wird in einem typischen Identity Manager-System, bei dem die Personaldatenbank die autorisierte Quelle für die meisten Mitarbeiterdaten ist, durch das Hinzufügen eines Mitarbeiters zur Personaldatenbank die automatische Erstellung eines entsprechenden Kontos im Identitätsdepot veranlasst. Die Erstellung des Kontos im Identitätsdepot veranlasst wiederum die automatische Erstellung eines Email-Kontos für den Mitarbeiter im Email-System. Die zur Bereitstellung des Kontos im Email-System verwendeten Daten werden aus dem Identitätsdepot abgerufen und können den Namen des Mitarbeiters, den Standort, die Telefonnummer usw. umfassen.

Die automatische Bereitstellung von Konten, Zugriffsrechten und Daten kann auf verschiedene Weisen gesteuert werden:

- *Datenelementwerte*: Die automatische Erstellung eines Kontos in den Zugriffsdatenbanken für verschiedene Gebäude kann beispielsweise durch einen Wert im Standortattribut eines Mitarbeiters gesteuert werden.
- *Genehmigungsworkflows*: Die Erstellung eines Mitarbeiters in der Finanzabteilung kann beispielsweise eine automatische Email an den Abteilungsleiter mit der Anforderung einer Genehmigung für ein neues Mitarbeiterkonto im Finanzsystem veranlassen. Der Abteilungsleiter wird über die Email auf eine Webseite geleitet, auf der er die Anforderung genehmigen oder ablehnen kann. Die Genehmigung kann dann die automatische Erstellung eines Kontos für den Mitarbeiter im Finanzsystem veranlassen.
- *Rollenzuweisungen*: Ein Mitarbeiter erhält beispielsweise die Rolle „Buchhalter“. Identity Manager stellt für den Mitarbeiter alle Konten, Zugriffsrechte und Daten bereit, die der Rolle „Buchhalter“ zugewiesen sind. Dies erfolgt über Systemworkflows (ohne menschliches Eingreifen), von Mitarbeitern durchgeführte Genehmigungsabläufe oder eine Kombination aus beidem.

Berechtigungen: Eine Berechtigung repräsentiert eine Ressource in einem verbundenen System, beispielsweise ein Konto oder eine Gruppenmitgliedschaft. Wenn ein Benutzer die Kriterien erfüllt, die für eine Berechtigung in einem verbundenen System festgelegt wurden, verarbeitet Identity Manager ein Ereignis für den Benutzer, mit dem Ergebnis, dass dem Benutzer Zugriff auf die Ressource gewährt wird. Dies erfordert natürlich, dass alle Richtlinien wirksam sind, damit der Zugriff auf die Ressource möglich ist. Wenn zum Beispiel ein Benutzer die Kriterien für ein Exchange-Konto in Active Directory erfüllt, verarbeitet die Metaverzeichnis-Engine den Benutzer mit den Active Directory-Treiberrichtlinien, die ein Exchange-Konto bereitstellen.

Der Hauptnutzen von Berechtigungen besteht darin, dass Sie die Geschäftslogik für den Zugriff auf eine Ressource in einer Berechtigung statt in mehreren Treiberrichtlinien definieren können. Zum Beispiel können Sie eine Kontoberechtigung definieren, die einem Benutzer in vier verbundenen Systemen ein Konto zur Verfügung stellt. Die Entscheidung, ob für den Benutzer ein Konto bereitgestellt werden soll, wird durch die Berechtigung getroffen, was bedeutet, dass die Richtlinien für die einzelnen vier Treiber die Geschäftslogik nicht enthalten müssen. Stattdessen müssen die Richtlinien nur den Mechanismus für die Gewährung des Kontos liefern. Wenn Sie eine Änderung an der Geschäftslogik vornehmen müssen, führen Sie dies in der Berechtigung aus und nicht in den einzelnen Treibern.

Aufträge: Die meisten Aktionen, die Identity Manager ausführt, erfolgen als Reaktion auf Datenänderungen oder Benutzeranforderungen. Wenn beispielsweise Daten in einem System geändert werden, ändert Identity Manager die entsprechenden Daten in einem anderen System. Wenn ein Benutzer Zugriff auf ein System anfordert, initiiert Identity Manager die entsprechenden Prozesse (Workflows, Ressourcenbereitstellung usw.) für die Gewährung des Zugriffs.

Aufträge ermöglichen Identity Manager das Ausführen von Aktionen, die nicht durch Datenänderungen oder Benutzeranforderungen initiiert werden. Ein Auftrag besteht aus Konfigurationsdaten, die im Identitätsdepot gespeichert sind, und einem entsprechenden Implementierungscode. Identity Manager enthält vordefinierte Aufträge, die Aktionen wie das Starten oder Anhalten von Treibern, das Senden von Email-Benachrichtigungen über ablaufende Passwörter und das Prüfen des Zustands von Treibern ausführen. Sie können auch benutzerdefinierte Aufträge zur Durchführung weiterer Aktionen implementieren. Für einen benutzerdefinierten Auftrag müssen Sie (bzw. ein Entwickler oder Berater) den für die Durchführung der gewünschten Aktionen erforderlichen Code erstellen.

Aufträge: In der Regel werden Änderungen an Daten im Identitätsdepot oder in einer verbundenen Anwendung sofort verarbeitet. Mithilfe von Aufträgen können Sie Aufgaben planen, die an einem bestimmten Datum und zu einer bestimmten Uhrzeit ausgeführt werden sollen. Zum Beispiel wird ein neuer Mitarbeiter eingestellt, der jedoch erst im nächsten Monat bei dem Unternehmen anfängt. Der Mitarbeiter muss zur Personaldatenbank hinzugefügt werden, er soll jedoch erst ab seinem ersten Arbeitstag Zugriff auf die Ressourcen des Unternehmens (Email, Server usw.) erhalten. Ohne die Verwendung eines Auftrags würde der Benutzer den Zugriff sofort erhalten. Wenn Aufträge implementiert sind, wird ein Auftrag erstellt, der die Kontobereitstellung erst am ersten Arbeitstag des Mitarbeiters initiiert.

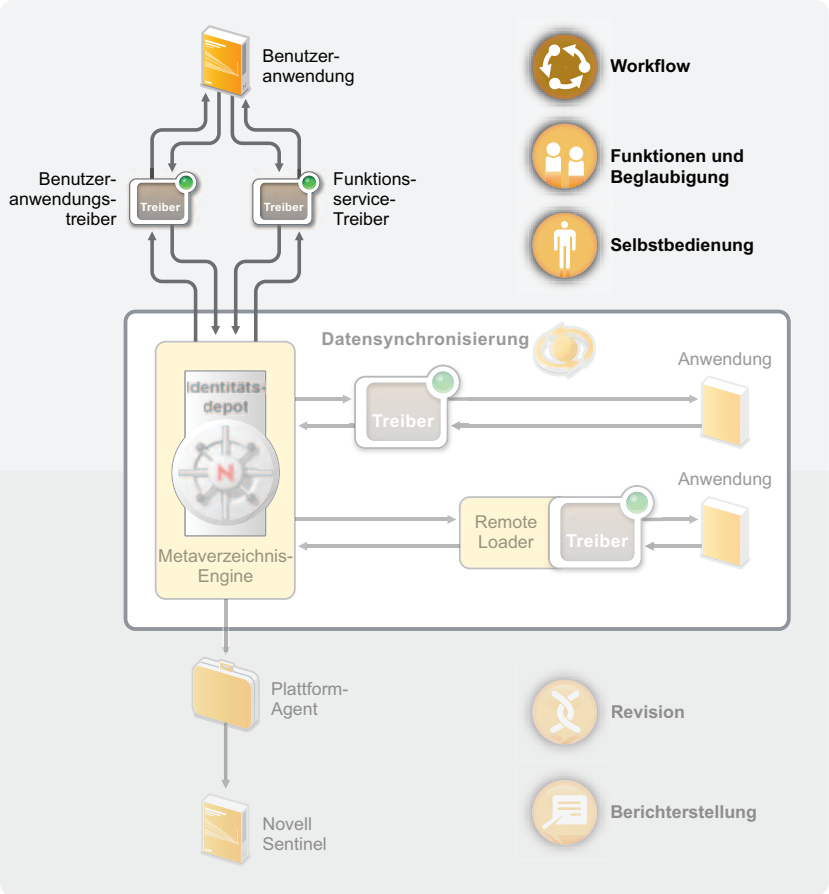
2.2 Workflow, Rollen, Beglaubigung und Selbstbedienung

Identity Manager bietet eine spezialisierte Anwendung, die Benutzeranwendung, die Genehmigungsworkflows, Rollenzuweisungen, die Beglaubigung und die Identitätsselbstbedienung ermöglicht.

Die Standard-Benutzeranwendung ist in Identity Manager enthalten. Die Standardversion bietet die Passwortselbstbedienung, mit deren Hilfe Benutzer vergessene Passwörter wiedererlangen oder zurücksetzen können, Organigramme für die Verwaltung von Benutzerverzeichnisinformationen, Benutzerverwaltungsfunktionen, die das Erstellen von Benutzern im Identitätsdepot ermöglichen, sowie Grundfunktionen der Identitätsselbstbedienung wie das Verwalten von Benutzerprofilinformationen.

Das rollenbasierte Bereitstellungsmodul der Benutzeranwendung ist ein separat erhältliches Zusatzmodul für Identity Manager. Wenn Sie das rollenbasierte Bereitstellungsmodul hinzufügen, stehen Ihnen über die Funktionen der Standard-Benutzeranwendung hinaus die erweiterte Selbstbedienung, der Genehmigungsworkflow, die rollenbasierte Bereitstellung, Funktionstrennungsbeschränkungen und die Beglaubigung zur Verfügung.

Abbildung 2-3 *Identity Manager-Benutzeranwendung*



In den folgenden Abschnitten finden Sie Beschreibungen dieser Komponenten sowie Erläuterungen der Konzepte, die Sie verstehen sollten, um die Komponenten erfolgreich implementieren und verwalten zu können:

- Abschnitt 2.2.1, „Komponenten“, auf Seite 25
- Abschnitt 2.2.2, „Wichtige Konzepte“, auf Seite 26

2.2.1 Komponenten

Benutzeranwendung: Die Benutzeranwendung ist eine browserbasierte Webanwendung, die Benutzern und Geschäftsadministratoren die Möglichkeit bietet, verschiedene Identitätsselbstbedienungs- und Rollenbereitstellungsaufgaben auszuführen, z. B. das Verwalten von Passwörtern und Identitätsdaten, das Initiieren und Überwachen von Bereitstellungs- und Rollenzuweisungsanforderungen, das Verwalten des Genehmigungsverfahrens für Bereitstellungsanforderungen und das Prüfen von Beglaubigungsberichten. Sie beinhaltet die Workflow-Engine, die die Weiterleitung von Anforderungen im Rahmen des entsprechenden Genehmigungsverfahrens steuert.

Benutzeranwendungstreiber: Der Benutzeranwendungstreiber speichert Konfigurationsinformationen und benachrichtigt die Benutzeranwendung über Änderungen im Identitätsdepot. Er kann darüber hinaus so konfiguriert werden, dass er das Auslösen von

Workflows durch Ereignisse zulässt, und dass er der Benutzeranwendung den Erfolg oder das Fehlschlagen der Bereitstellungsaktivität eines Workflows meldet, sodass Benutzer den endgültigen Status ihrer Anforderungen sehen können.

Rollenservice-Treiber: Der Rollenservice-Treiber verwaltet alle Rollenzuweisungen, startet Workflows für Rollenzuweisungsanforderungen, die eine Genehmigung erfordern, und verwaltet indirekte Rollenzuweisungen nach Gruppen- und Containermitgliedschaften. Der Treiber erteilt und entzieht Berechtigungen für Benutzer basierend auf ihren Rollenmitgliedschaften und führt Bereinigungsprozeduren für abgeschlossene Anforderungen durch.

2.2.2 Wichtige Konzepte

Workflow-basierte Bereitstellung: Die Workflow-basierte Bereitstellung bietet den Benutzern die Möglichkeit, Zugriff auf Ressourcen anzufordern. Eine Bereitstellungsanforderung wird durch einen vordefinierten Workflow weitergeleitet, der möglicherweise die Genehmigung durch eine oder mehrere Personen beinhaltet. Wenn alle Genehmigungen erteilt wurden, erhält der Benutzer Zugriff auf die Ressource. Bereitstellungsanforderungen können auch indirekt als Reaktion auf Ereignisse im Identitätsdepot initiiert werden. Zum Beispiel kann durch das Hinzufügen eines Benutzers zu einer Gruppe eine Anforderung für die Erteilung des Zugriffs auf eine bestimmte Ressource für den Benutzer initiiert werden.

Rollenbasierte Bereitstellung: Die rollenbasierte Bereitstellung ermöglicht, dass Benutzer auf der Grundlage der ihnen zugewiesenen Rollen Zugriff auf bestimmte Ressourcen erhalten. Benutzern können eine oder mehrere Rollen zugewiesen werden. Wenn eine Rollenzuweisung eine Genehmigung erfordert, startet die Zuweisungsanforderung einen Workflow.

Funktionstrennung: Damit Benutzern keine widersprüchlichen Rollen zugewiesen werden, bietet das rollenbasierte Bereitstellungsmodul der Benutzeranwendung die Möglichkeit der Funktionstrennung. Sie können *Funktionstrennungsbeschränkungen* einrichten, die definieren, welche Rollen als widersprüchlich zueinander angesehen werden. Wenn Rollen im Widerspruch zueinander stehen, haben *Funktionstrennungsgenehmiger* die Möglichkeit, *Ausnahmen* von den Beschränkungen zu genehmigen oder zu verweigern. Genehmigte Ausnahmen werden als *Funktionstrennungsverletzungen* aufgezeichnet und können mithilfe des nachfolgend beschriebenen Beglaubigungsprozesses überprüft werden.

Rollenverwaltung: Die Rollen müssen von Mitarbeitern verwaltet werden, denen die Systemrollen *Rollenmodul-Administrator* und *Rollenmanager* zugewiesen wurden.

Der Rollenmodul-Administrator kann neue Rollen erstellen, vorhandene Rollen ändern, Rollen entfernen, Beziehungen zwischen Rollen ändern, Rollenzuweisungen für Benutzer erteilen und entziehen sowie Funktionstrennungsbeschränkungen erstellen, ändern und entfernen.

Der Rollenmanager kann dieselben Aufgaben durchführen wie der Rollenmodul-Administrator, mit Ausnahme des Verwaltens von Funktionstrennungsbeschränkungen, der Konfiguration des Rollensystems und des Ausführens aller Berichte. Außerdem bestehen für den Rollenmodul-Administrator keine Bereichsbeschränkungen innerhalb des Rollensystems, während der Bereich des Rollenmanagers auf speziell ausgewiesene Benutzer, Gruppen und Rollen beschränkt ist.

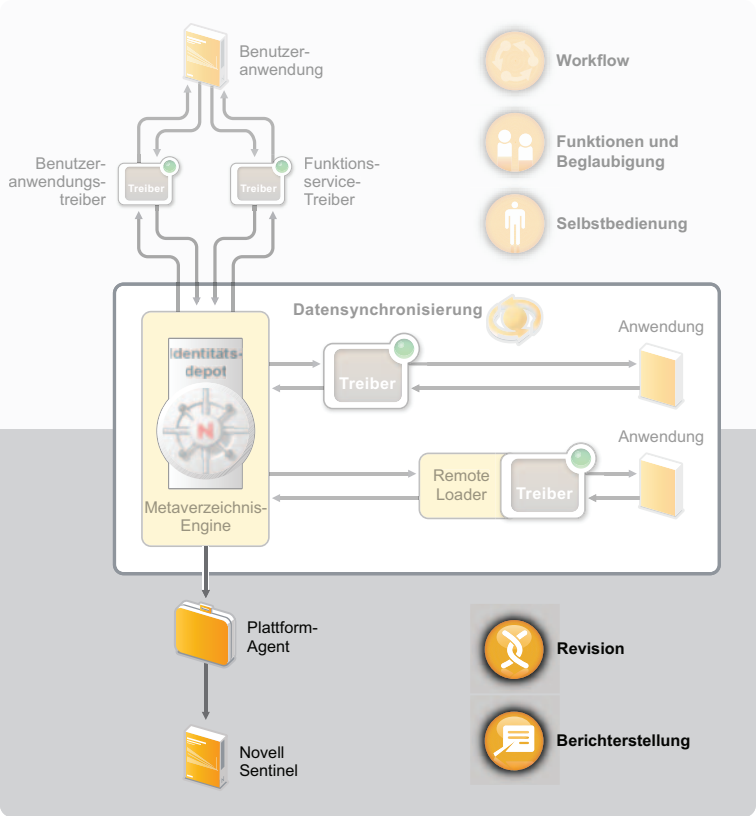
Beglaubigung: Rollenzuweisungen bestimmen den Zugriff eines Benutzers auf Ressourcen innerhalb Ihrer Organisation. Falsche Zuweisungen können die Einhaltung von Unternehmens- und behördlichen Bestimmungen gefährden. Mit Identity Manager können Sie die Richtigkeit von

Rollenzuweisungen durch einen Beglaubigungsprozess validieren. Dieser Prozess ermöglicht einzelnen Benutzern das Überprüfen ihrer eigenen Profilinformationen und Rollenmanagern die Validierung von Rollenzuweisungen und Funktionstrennungsverletzungen.

2.3 Revision und Berichterstellung

Die Revision und die Berichterstellung werden durch die Integration mit Novell Sentinel™ ermöglicht, wie im folgenden Diagramm dargestellt.

Abbildung 2-4 *Revision und Berichterstellung in Identity Manager*



Plattformagent: Der Plattformagent erfasst Ereignisse aus der Metaverzeichnis-Engine und sendet diese an das Novell Sentinel-System.

Novell Sentinel: Novell Sentinel ist eine Sicherheitsinformations- und Ereignismanagement-Lösung (SIEM), die das Sammeln, die Analyse und die Berichterstellung von Systemnetzwerk-, Anwendungs- und Sicherheitsprotokollen automatisiert. Novell Sentinel ist separat erhältlich.

Eine umfassende Einführung zu Novell Sentinel und Hinweise zum Kauf finden Sie auf der Novell Sentinel-Website (http://www.novell.com/products/sentinel/).

Identity Manager-Werkzeuge

3

Identity Manager bietet drei grundlegende Werkzeuge, die Sie beim Einrichten und Verwalten Ihres Identity Manager-Systems unterstützen: Designer, iManager und die Benutzeranwendungs-Administrationskonsole.

Mithilfe von Designer können Sie Ihr Identity Manager-System in einer Offline-Umgebung erstellen und konfigurieren und Ihre Änderungen dann in Ihr Live-System übertragen. Mit iManager können Sie dieselben Aufgaben ausführen wie mit Designer und außerdem den Zustand Ihres Systems überwachen. Änderungen, die Sie in iManager vornehmen, werden jedoch sofort wirksam, daher wird empfohlen, iManager für einfache Administrationsaufgaben und Designer für komplexere Konfigurationsaufgaben zu verwenden, die ein Modellieren und Testen vor der Bereitstellung erfordern.

Mithilfe der Benutzeranwendungs-Administrationskonsole können Sie das Erscheinungsbild der Anwendung verwalten, indem Sie Seiten und Portlets erstellen und ändern. Außerdem können Sie Anwendungseinstellungen wie z. B. Caching- und Protokollierungseinstellungen ändern und spezifische Delegierungs- und Vertretungseinstellungen für die Bereitstellungsfunktion der Benutzeranwendung konfigurieren.

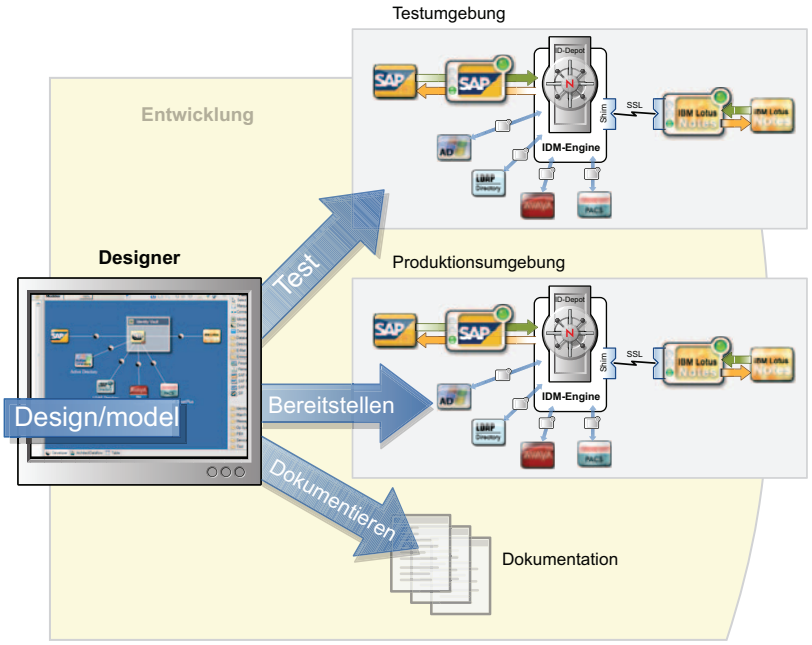
In den folgenden Abschnitten finden Sie weitere Informationen zu den einzelnen Werkzeugen:

- Abschnitt 3.1, „Designer“, auf Seite 29
- Abschnitt 3.2, „iManager“, auf Seite 30
- Abschnitt 3.3, „Administrationskonsole der Benutzeranwendung“, auf Seite 31

3.1 Designer

Designer ist ein Eclipse*-basiertes Werkzeug, das Sie beim Entwerfen, Bereitstellen und Dokumentieren Ihres Identity Manager-Systems unterstützt. Mit der grafischen Schnittstelle von Designer können Sie Ihr System in einer Offline-Umgebung entwerfen und testen, das System in Ihrer Produktionsumgebung bereitstellen und alle Details Ihres bereitgestellten Systems dokumentieren.

Abbildung 3-1 *Designer für Identity Manager*



Es ist zwar möglich, ein Identity Manager-System ohne Designer einzurichten, dies ist jedoch deutlich schwieriger und wird nicht empfohlen.

Entwerfen: Designer bietet eine grafische Schnittstelle, über die Sie Ihr System modellieren können. Dabei stehen Ansichten zur Verfügung, in denen Sie die Verbindungen zwischen Identity Manager und Anwendungen erstellen und steuern, Richtlinien konfigurieren und den Datenfluss zwischen verbundenen Anwendungen manipulieren können.

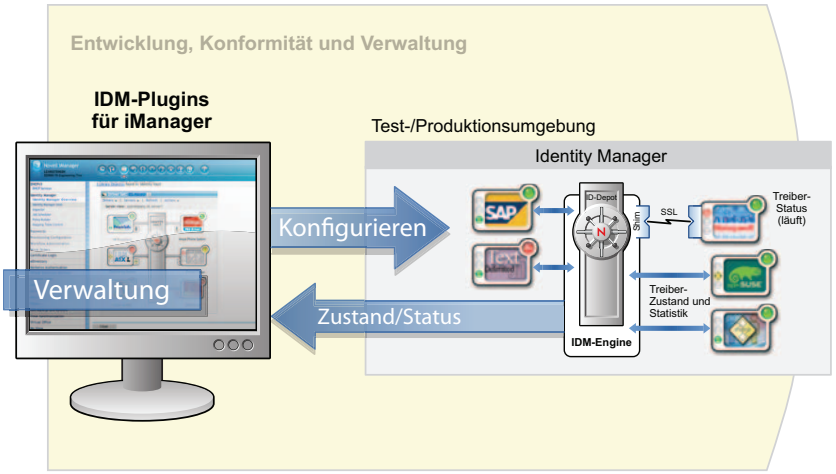
Bereitstellen: Ihre in Designer ausgeführte Arbeit wird erst dann in Ihrer Produktionsumgebung bereitgestellt, wenn Sie die Bereitstellung initiieren. Dadurch besitzen Sie die Freiheit, zu experimentieren, die Ergebnisse zu testen und Probleme zu beheben, bevor das System in Ihrer Produktionsumgebung eingesetzt wird.

Dokument: Sie können umfangreiche eine Dokumentation generieren, die Ihre Systemhierarchie, Treiberkonfigurationen, Richtlinienkonfigurationen und vieles mehr darstellt. Sie erhalten dadurch alle Informationen, die zum Verständnis der technischen Aspekte Ihres Systems erforderlich sind, und die Überprüfung der Konformität mit Ihren geschäftlichen Regeln und Richtlinien wird vereinfacht.

3.2 iManager

Novell® iManager ist ein browserbasiertes Werkzeug, das einen einzelnen Administrationspunkt für viele Novell-Produkte, einschließlich Identity Manager, zur Verfügung stellt. Mithilfe der Identity Manager-Plugins für iManager können Sie Identity Manager verwalten und Echtzeitinformationen zum Zustand und Status Ihres Identity Manager-Systems erhalten.

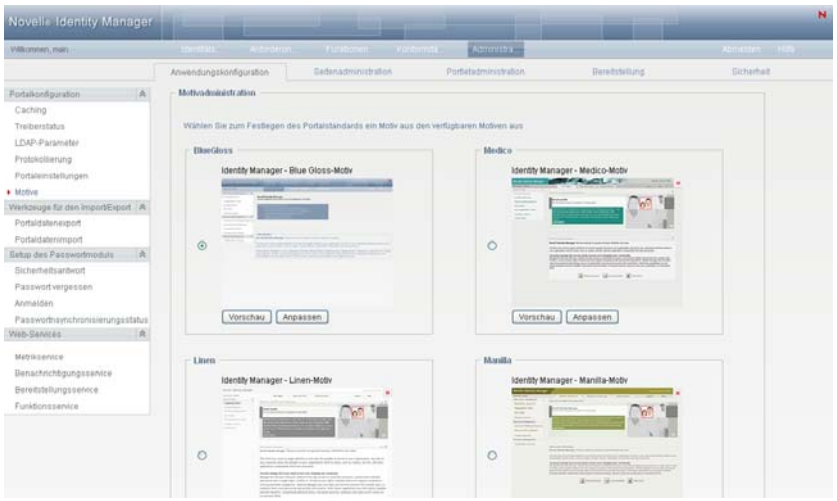
Abbildung 3-2 *Novell iManager*



3.3 Administrationskonsole der Benutzeranwendung

Die Benutzeranwendung stellt eine webbasierte Verwaltungskonsole zur Verfügung, mit deren Hilfe Sie die Passwortselbstbedienung, die Rollen und die Bereitstellung konfigurieren, verwalten und anpassen können. Die Administrationskonsole wird für alle Benutzer, denen Administratorrechte zugewiesen wurden, in der Benutzeranwendung als Registerkarte *Administration* hinzugefügt.

Abbildung 3-3 *Administrationsseiten der Benutzeranwendung*



Auf der Administrationsseite der Benutzeranwendung befinden sich die folgenden Registerkarten:

- **Anwendungskonfiguration:** Hier können Sie das Caching, die LDAP-Parameter, die Protokollierung, die Motive und das Setup des Passwortmoduls konfigurieren.
- **Seitenadministration:** Hier können Sie neue Seiten erstellen und vorhandene Identitätsselbstbedienungsseiten anpassen.
- **Portletadministration:** Hier können Sie neue Portlets erstellen und die vorhandenen Portlets anpassen, die auf den Identitätsselbstbedienungsseiten verwendet werden.

- **Bereitstellung:** Hier können Sie die Delegierung, die Vertretung, Aufgaben, den Digitalsignaturservice sowie Engine- und Clustereinstellungen konfigurieren.
- **Sicherheit:** Hier können Sie definieren, welche Benutzer Bereitstellungsadministrator- und Benutzeranwendungsadministratorrechte besitzen sollen.