Übersichtshandbuch

Novell®
Identity Manager

4.0.1

15. April 2011

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.
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

Dieses Handbuch bietet eine Einführung in Novell Identity Manager, ein WorkloadIQ-Produkt, das die Verwaltung von Identitäten und Zugriffen in physischen, virtuellen sowie Cloud-Umgebungen ermöglicht. Es wird erläutert, wie Sie Geschäftsprobleme mithilfe von Identity Manager lösen und gleichzeitig Kosten einsparen sowie die Konformität sicherstellen können. Das Handbuch enthält außerdem einen technischen Überblick über die Komponenten und Werkzeuge von Identity Manager, die zum Erstellen Ihrer Identity Manager-Lösung zur Verfügung stehen. 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 der Dokumentation

Die neueste Version dieses Dokuments finden Sie auf der Website zur Identity Manager-Dokumentation (http://www.novell.com/documentation/idm401/index.html).

Zusätzliche Dokumentation

Die Dokumentation für Identity Manager-Treiber finden Sie auf der Website für Identity Manager-Treiber (http://www.novell.com/documentation/idm401drivers/index.html).

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 4, „Identity Manager-Architektur“, auf Seite 27 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 „Workflows“, „Rollen“, „Beglaubigung“, „Selbstbedienung“, „Revision“ und „Berichterstellung“ verwenden die durch Ihre Geschäftsrichtlinien gesteuerte Datensynchronisierung zwischen mehreren Systemen, um die Prozesse zu automatisieren, 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:

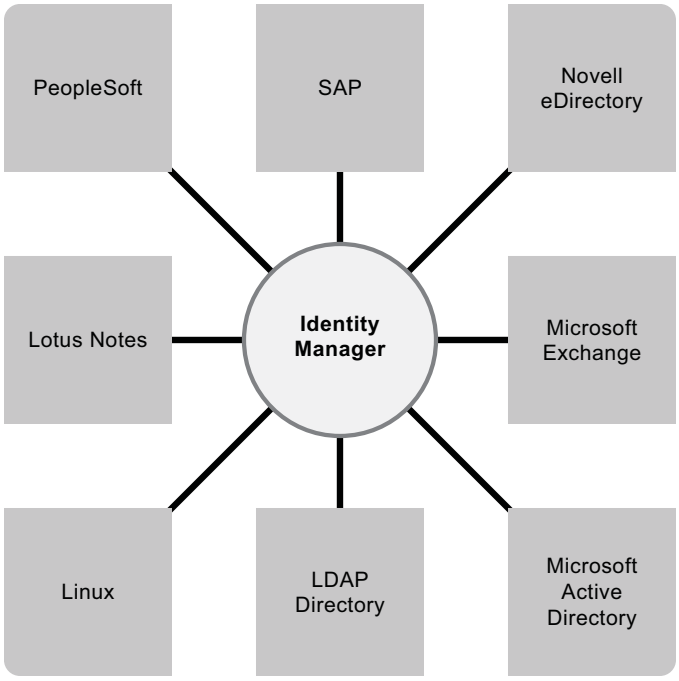
- Abschnitt 1.1, „Datensynchronisierung“, auf Seite 8
- Abschnitt 1.2, „Workflow“, auf Seite 11
- Abschnitt 1.3, „Rollen und Beglaubigung“, auf Seite 12
- Abschnitt 1.4, „Selbstbedienung“, auf Seite 14
- Abschnitt 1.5, „Revision, Berichterstellung und Konformität“, auf Seite 15

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 eine Vielzahl an Anwendungen, Datenbanken, Betriebssystemen und Verzeichnissen hinweg synchronisieren, transformieren und verteilen, z. B. Daten aus SAP, PeopleSoft, Salesforce, Microsoft SharePoint, Lotus Notes, Microsoft Exchange, Microsoft Active Directory, Novell eDirectory, Linux und UNIX sowie LDAP-Verzeichnissen.

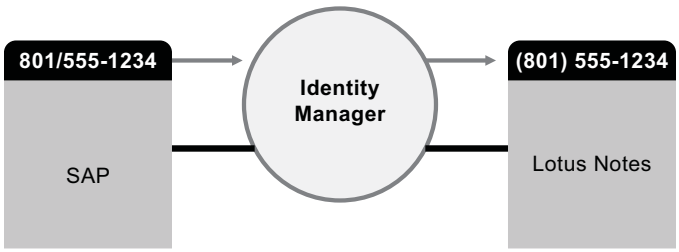
Abbildung 1-2 *Verbinden mehrerer Systeme mit Identity Manager*



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.

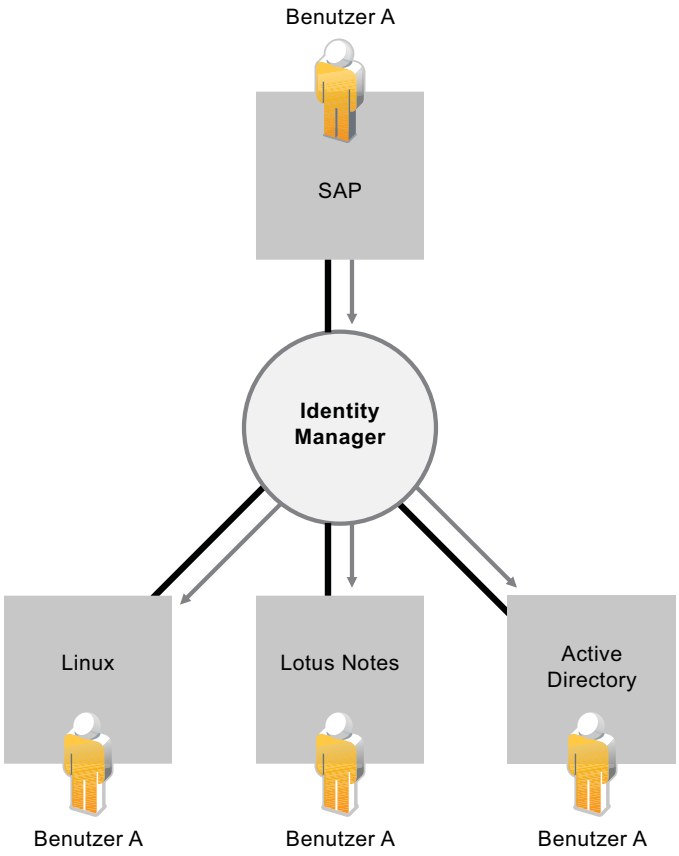
Im nachfolgenden Diagramm ist die SAP-Personaldatenbank die autorisierte Quelle für die Telefonnummer eines Benutzers. Das Lotus Notes-System verwendet ebenfalls Telefonnummern, daher wandelt Identity Manager die Nummer in das erforderliche Format um und überträgt sie an das Lotus Notes-System. Jedes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

Abbildung 1-3 *Datensynchronisierung verbundener Systeme*



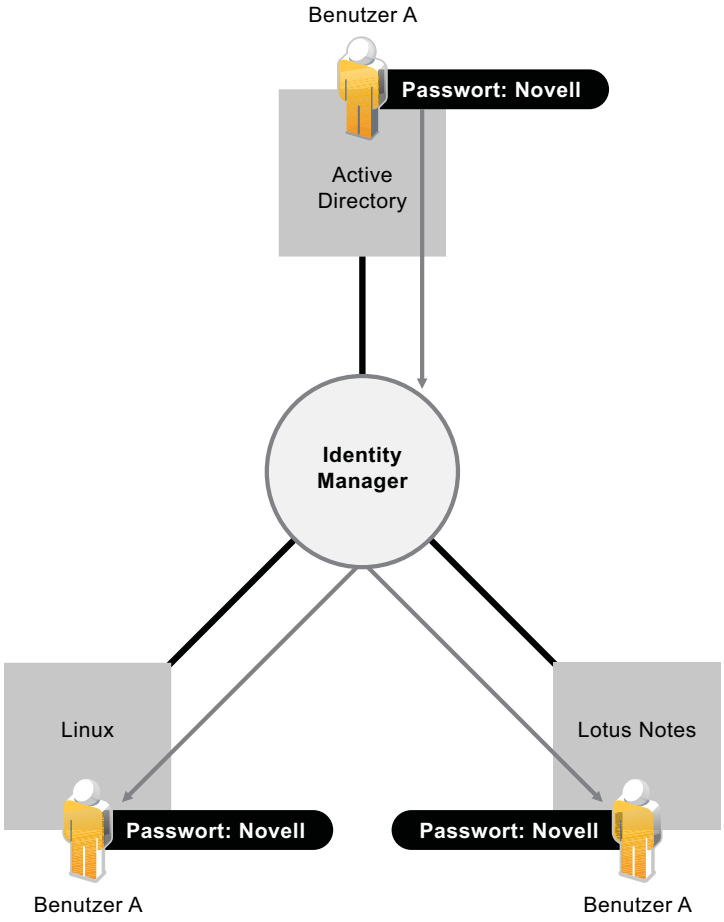
Das Verwalten der Daten vorhandener Benutzer stellt nur die erste Ebene der Datensynchronisierungsfunktionen von Identity Manager dar. Zusätzlich können mit Identity Manager in Verzeichnissen wie Active Directory, auf Systemen wie PeopleSoft und Lotus Notes und unter Betriebssystemen wie UNIX und Linux 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*

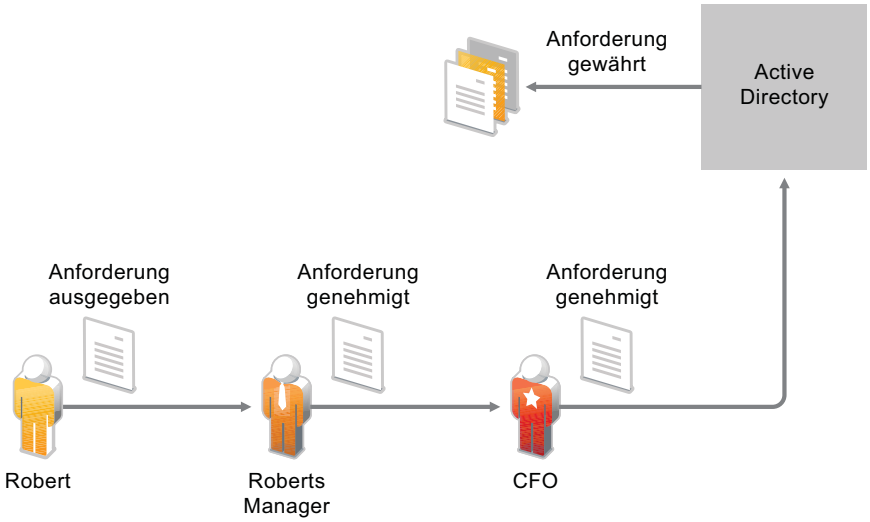


1.2 Workflow

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*



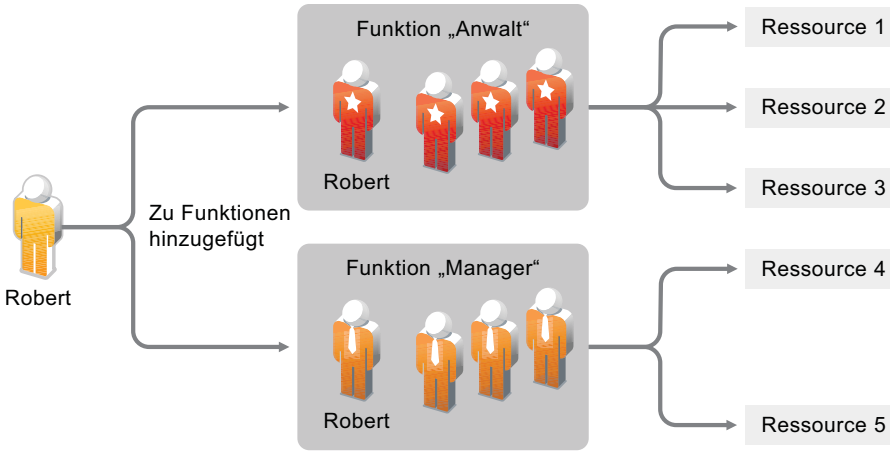
Workflows können automatisch initiiert werden, sobald ein bestimmtes Ereignis eintritt (z. B. wenn ein neuer Benutzer zu Ihrem Personalsystem hinzugefügt wird), oder sie können manuell durch eine Benutzeranforderung initiiert werden. Sie können sicherstellen, dass Genehmigungen rechtzeitig erteilt werden,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

1.3 Rollen und Beglaubigung

Oft hängt es von der Funktion 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

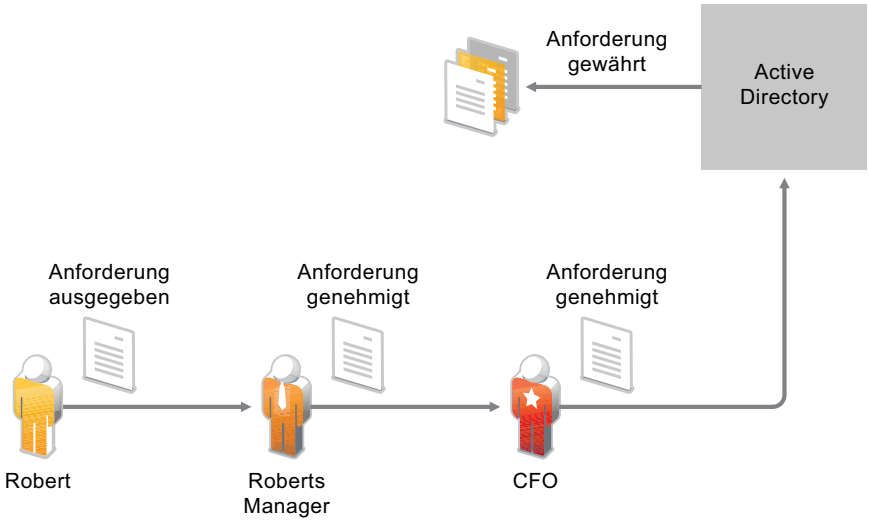
Vermutlich gibt es bei Ihnen Vorgesetzte und Abteilungen, die ihre Benutzerinformationen und Zugriffsanforderungen lieber selbst verwalten würden, als dies Ihnen oder Ihren Mitarbeitern zu überlassen. Wie oft haben Sie schon Sätze gehört wie, „Warum kann ich meine Handynummer in unserem Unternehmensverzeichnis 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 11 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, Berichterstellung und Konformität

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 - vorangegangene und aktuelle - verfolgt und zu Revisionszwecken protokolliert werden. Identity Manager verfügt über ein intelligentes Repository mit Informationen über den aktuellen und den gewünschten Status des Identitätsdepots sowie der verwalteten Systeme in Ihrer Organisation. Aus diesem Warehouse können Sie jederzeit alle Informationen abrufen, die für die Einhaltung der für Ihre Organisation geltenden geschäftlichen Regeln und Richtlinien erforderlich sind.

Das Warehouse gibt Ihnen einen Gesamtüberblick über alle Geschäftsberechtigungen und Aufschluss darüber, welche Autorisierungen und Berechtigungen den Identitäten in Ihrer Organisation in der Vergangenheit und gegenwärtig erteilt wurden. Somit haben Sie die Gewissheit, dass Sie für die Einhaltung selbst anspruchsvollster GRC-Richtlinien gerüstet sind.

Identity Manager enthält vordefinierte Berichte für Identitätsinformations-Warehouse-Abfragen zur Sicherstellung der Einhaltung von Geschäfts-, IT- und Firmenrichtlinien. Sie können auch benutzerdefinierte Berichte erstellen, falls die vordefinierten Berichte für Ihre Anforderungen nicht geeignet sind.

Funktionen von Identity Manager 4.0.1

2

Novell Identity Manager 4.0.1 bietet ein intelligentes Identity-Framework, das Ihre vorhandenen IT-Assets und neue Computing-Modelle, z. B. „Software As a Service (SaaS)“, nutzt und somit Kosteneinsparungen ermöglicht sowie die Konformität zwischen physischen, virtuellen und Cloud-Umgebungen sicherstellt. Mithilfe von Novell Identity Manager-Lösungen können Sie sicherstellen, dass Ihre Organisation über die aktuellsten Benutzeridentitätsinformationen verfügt. Sie behalten die Kontrolle auf Unternehmensebene, indem Sie Identitäten innerhalb der Firewall und cloud-übergreifend verwalten, bereitstellen bzw. die Bereitstellung aufheben. Identity Manager ermöglicht Ihnen, auch Clouds in die Konformitätsverwaltung mit einzubeziehen.

Identity Manager 4.0.1 ist mit umfassenden Funktionen zum Vorkonfigurieren und Anpassen der Identity Manager-Treiberrichtlinien ausgestattet. Hierzu gehören das Identitätsmanagement und die Rollenverwaltung sowie Berichterstellungs- und Paketverwaltungsfunktionen. Sie können darüber hinaus Sicherheitsrichtlinien auf mehrere Systemdomänen anwenden. Identity Manager ermöglicht Ihnen die Benutzerverwaltung bei einer wachsenden Zahl an behördlichen Regelungen und gesetzlichen Bestimmungen. Es bietet mehr Schutz durch strategische Benutzerbereitstellungen und erfüllt somit den wachsenden Sicherheitsbedarf innerhalb der Firewall und in der Cloud-Umgebung. Das intelligente Identity-Framework bietet die Möglichkeit, Ihre vorhandene Infrastruktur mit neuen Computing-Modellen wie SaaS zu kombinieren.

2.1 Neue Funktionen von Identity Manager 4.0.1

- **Aktivität „Ressourcenanforderung“:** Die Aktivität „Ressourcenanforderung“ ermöglicht Ihnen, das Zuweisen bzw. Entziehen von Ressourcen zu automatisieren. Beispielsweise können Sie eine Bereitstellungsanforderungsdefinition schreiben, die einem neuen Mitarbeiter an seinem ersten Arbeitstag alle benötigten Ressourcen bereitstellt. Mithilfe der Aktivität „Ressourcenanforderung“ können Sie die Genehmigung von bestimmten Ressourcen für diesen Mitarbeiter automatisieren. Ausführliche Informationen zur Aktivität „Ressourcenanforderung“ finden Sie unter „*Resource Request Activity*“ (Aktivität „Ressourcenanforderung“) im *User Application: Design Guide* (Designhandbuch zur Benutzeranwendung).
- **Telemetrie:** Identity Manager Telemetry ist ein neuer Auftrag, der in Identity Manager 4.0.1 eingeführt wurde. Der Auftrag kann als Zählprogramm für die Lizenznutzung und als Lizenzüberwachungswerkzeug eingesetzt werden. Mithilfe des Lizenzüberwachungswerkzeugs können Identity Manager-Kunden mehr Lizenzen hinzufügen oder nicht verwendete Lizenzen deaktivieren. Die Kunden können auch von Vorteilen wie z. B. der Preisgebung für inaktive Benutzer profitieren.

  Der Telemetrieauftrag sammelt Informationen zu den installierten Software- und Hardwarekomponenten von Identity Manager sowie zur Verwendung der Identity Manager-Treiber in der Kundenumgebung. Nachdem sich der Kunde beim Novell Customer Center registriert hat, werden die Informationen an Novell gesendet. Mithilfe der gesammelten Informationen kann Novell dem Kunden eine bessere Unterstützung bieten. Darüber hinaus

wird Identity Manager effektiver und effizienter weiterentwickelt und getestet und es können wichtige Entscheidungen für zukünftige Versionen getroffen werden. Weitere Informationen finden Sie im *Identity Manager 4.0.1 Jobs Guide* (Handbuch zu Identity Manager 4.0.1 Aufträgen).

- **Berichte:** Folgende Berichte wurden zum Identitätsberichterstellungsmodul hinzugefügt:
  - **Benutzerstatusänderung im Identitätsdepot:** Enthält für die Identitätsdepotbenutzer signifikante Ereignisse.
  - **Benutzerpasswortänderung im Identitätsdepot:** Zeigt alle Benutzerpasswortänderungen im Identitätsdepot an.
  - **Zugriffsanfragen nach Empfänger:** Enthält die Workflow-Prozesse zu Ressourcenzuweisungen gruppiert nach Empfänger.
  - **Zugriffsanfragen nach Anforderer:** Enthält die Workflow-Prozesse zu Ressourcenzuweisungen gruppiert nach Anforderer.
  - **Zugriffsanfragen nach Ressource:** Enthält die Workflow-Prozesse zu Ressourcenzuweisungen gruppiert nach Ressourcen.

2.2 Funktionen von Identity Manager 4.0

Neben den beschriebenen neuen Funktionen ist Identity Manager 4.0.1 mit den folgenden Funktionen ausgestattet, die in Identity Manager 4.0 hinzugefügt wurden.

- **Umfassende, sofort einsatzfähige Berichterstellung:** Mithilfe des integrierten Berichterstellungsmoduls von Novell Identity Manager 4.x lässt sich die Konformität von In-House- und Cloud-Bereitstellungen besser darstellen. Mit den Berichterstellungsfunktionen können Sie die Benutzerrechte und den Identitätsstatus eines bestimmten Benutzers anzeigen oder einen Bereitstellungsverlauf und einen Bericht über die vom Benutzer durchgeführten Aktionen erstellen. Weitere Informationen hierzu finden Sie im *Identity Reporting Module Guide* (Handbuch zum Identitätsberichterstellungsmodul).
- **Erweiterte Integration:** Zum Erstellen einer neuen Identity Manager-Lösung, in der sich alle Komponenten auf demselben Server befinden, bietet Ihnen Novell Identity Manager 4.x ein integriertes Installationsprogramm, das die Installation erleichtert und mit dem Sie Ihr System schneller einrichten können. Anstatt die Identity Manager-Komponenten einzeln zu installieren, können Sie mithilfe des integrierten Installationsprogramms alle Komponenten in einem Installationsvorgang installieren. Weitere Informationen finden Sie im *Identity Manager 4.0.1 Integrated Installation Guide* (Handbuch zur integrierten Installation von Identity Manager 4.0).
- **Paketverwaltung:** Identity Manager 4.x bietet das neue Konzept „Paketverwaltung“. Dieses System dient zum Erstellen, Verteilen und Verwenden von hochwertigen Bausteinen mit Identity Manager-Richtlinieninhalten. Weitere Informationen zu Identity Manager-Paketen finden Sie unter *Configuring Packages* (Konfigurieren von Paketen) im *Designer 4.0.1 for Identity Manager 4.0.1 Administration Guide* (Administrationshandbuch zu Designer 4.0.1 für Identity Manager 4.0.1).
- **Cloud-fähige Treiber:** Identity Manager 4.x bietet mehrere Treiber für die Integration in SaaS. Die Treiber lassen sich nahtlos in SaaS und die gehostete Lösung integrieren und bieten unter anderem folgende Funktionen: Bereitstellung, Deaktivierung der Bereitstellung, Anforderungs- bzw. Genehmigungsverfahren, Passwortänderungen, Identitätsprofilaktualisierungen und Berichterstellung. Mithilfe der Treiber „New SharePoint“ und „Salesforce.com“ können Sie Ihre Unternehmensidentitäten in Cloud-Anwendungen integrieren. Weitere Informationen zu

cloud-fähigen Treibern finden Sie im *Identity Manager 4.0.1 Driver for Salesforce.com Implementation Guide* (Implementierungshandbuch für Identity Manager 4.0.1-Treiber für Salesforce.com) und im *Identity Manager 4.0.1 Driver for SharePoint Implementation Guide* (Implementierungshandbuch für Identity Manager 4.0.1-Treiber für SharePoint).

- **Eingebettetes Identitätsdepot:** Die Architektur von Novell Identity Manager 4.x umfasst ein optionales integriertes Identitätsdepot, wodurch das Erstellen und Verwalten einer separaten Verzeichnisstruktur für Identitätszwecke nicht mehr erforderlich ist. Zu den weiteren Ausstattungsmerkmalen der Novell Identity Manager 4.x-Produktfamilie gehören Treiber, die eine problemlose Integration des Identitätsdepots in andere Repositorys mit Identitätsinformationen, z. B. Active Directory oder verschiedene Datenbanken in Ihrem Unternehmen, ermöglichen. Weitere Informationen finden Sie im *Identity Manager 4.0.1 Integrated Installation Guide* (Handbuch zur integrierten Installation von Identity Manager 4.0).
- **Vereinfachte Identitäts- und Rollenverwaltung:** Die Novell Identity Manager 4.x-Produktfamilie vereinfacht die Integration von unterschiedlichen Rollen-Repositorys in einen konsolidierten Speicherort, sodass Sie nicht unterschiedliche Identifikationsinformationsquellen verwalten müssen. Über die neue intuitive Benutzeroberfläche des Rollenzuordnungsadministrators können Sie in Novell Identity Manager 4.x sogar Rollen und Profile von Drittanbietern zuordnen. Weitere Informationen hierzu finden Sie im *Novell Identity Manager Role Mapping Administrator 4.0.1 User Guide* (Benutzerhandbuch zum Novell Identity Manager-Rollenzuordnungsadministrator 4.0.1).
- **Erweiterte Werkzeuge:** Designer ist ein wichtiges Werkzeug, das Ihnen umfassende Funktionen zum Entwerfen einer Identity Manager-Lösung bereitstellt, die auf Ihre Anforderungen zugeschnitten ist. In Designer 4.x wurden mehrere Funktionen verbessert bzw. erweitert. Welche Änderungen vorgenommen wurden, sehen Sie in der Liste unter *Neuheiten* (http://www.novell.com/documentation/designer401/resources/whatsnew/index.html). Weitere Informationen zu den Funktionen und der Verwaltung von Designer finden Sie im *Designer 4.0.1 for Identity Manager 4.0.1 Administration Guide* (Administrationshandbuch zu Designer 4.0.1 für Identity Manager 4.0.1). Darüber hinaus verfügt Identity Manager über ein Werkzeug, mit dem sich Daten einfacher analysieren und bereinigen lassen. Weitere Informationen hierzu finden Sie im *Analyzer 4.0.1 for Identity Manager Administration Guide* (Administrationshandbuch zu Analyzer 4.0.1 für Identity Manager).

Identity Manager-Familie

3

Die Identity Manager-Produktfamilie ist in drei Produktgruppen unterteilt, die auf die verschiedenen Kundenanforderungen zugeschnitten sind:

- Identity Manager Advanced Edition
- Identity Manager Standard Edition
- Compliance Management-Plattform

Die Identity Manager Advanced Edition enthält neben den Funktionen der Identity Manager Standard Edition noch zusätzliche Funktionen. Die Compliance Management-Plattform ist mit den Funktionen der Advanced und Standard Edition sowie zusätzlichen Werkzeugen ausgestattet.

Abbildung 3-1 *Identity Manager-Produktgruppen*

Eine Gegenüberstellung der Funktionen der Advanced und der Standard Edition von Identity Manager finden Sie im Versionenvergleich zu Identity Manager (http://www.novell.com/products/identitymanager/features/identitymanager-version-comparison.html).

- Abschnitt 3.1, „Identity Manager Advanced Edition“, auf Seite 22
- Abschnitt 3.2, „Identity Manager Standard Edition“, auf Seite 22
- Abschnitt 3.3, „Compliance Management-Plattform“, auf Seite 24
- Abschnitt 3.4, „Aktivieren der Standard und Advanced Edition von Identity Manager“, auf Seite 25

3.1 Identity Manager Advanced Edition

Die Identity Manager 4.0.1 Advanced Edition enthält einen vollständigen Satz an Funktionen zur Bereitstellung für Benutzer der Unternehmensklasse. Sie enthält die Identitätsselbstbedienungsfunktionen der Standard Edition sowie umfassende Funktionen für die Workflow-basierte Bereitstellung. Mithilfe der Advanced Edition können Sie Workflow-Genehmigungsverfahren initiieren sowie Rollen und Ressourcen bereitstellen und von den Vorteilen der Konformitätsfunktionen profitieren. Ein weiteres Ausstattungsmerkmal der Advanced Edition ist das Arbeits-Dashboard.

Identity Manager 4.0.1 Advanced Edition ist als separate ISO-Imagedatei erhältlich.

Hinweis: Außerdem ist eine 90-Tage-Testversion von Identity Manager 4.0.1 Advanced Edition verfügbar.

3.2 Identity Manager Standard Edition

Um die verschiedenen Kundenbedürfnisse zu erfüllen, hat Novell Identity Manager 4.0.1 Standard Edition auf den Markt gebracht. Die Standard Edition enthält einen Teil der Funktionen der Identity Manager Advanced Edition.

Die Standard Edition bietet auch weiterhin alle Funktionen, die in älteren Versionen von Identity Manager vorhanden sind:

- Identitätsynchronisierung
- Automatische regelbasierte Bereitstellung
- Passwortverwaltung und Passwortselbstbedienung
- Identitätsselbstbedienung mit vorhandenen White Pages und Organigrammfunktionen

  ---

  Hinweis: Beide Identity Manager-Ausführungen (Advanced und Standard) enthalten weiterhin die gleichen Integrationsmodule.

Zusätzlich zu den oben aufgeführten Funktionen umfasst die Standard Edition die folgenden Funktionen der Advanced Edition:

- Erscheinungsbild der Benutzeroberfläche
- Berichterstellungsmodul
- Framework zum Verpacken von Inhalten
- Unterstützung für REST-APIs und Single Sign-on (SSO)
- Analyzer-Werkzeug für den Datenabgleich

Identity Manager 4.0.1 Standard Edition steht als separate ISO-Imagedatei zum Download zur Verfügung. Wenn Sie von der Standard Edition zur Advanced Edition aufrüsten möchten, verwenden Sie die Identity Manager Advanced Edition-ISO-Imagedatei. Sie müssen die richtige Aktivierung anwenden, um auf die Advanced Edition aufrüsten zu können. Weitere Informationen zum Aufrüsten der Standard Edition auf die Advanced Edition finden Sie im *Identity Manager 4.0.1 Upgrade and Migration Guide* (Aufrüstungs- und Migrationshandbuch zu Identity Manager 4.0.1).

Es ist nicht möglich, von einer installierten Identity Manager Advanced Edition zur Standard Edition zu wechseln, indem Sie die ISO-Imagedatei der Standard Edition verwenden. Wenn Sie von der Identity Manager Advanced Edition zur Standard Edition wechseln möchten, deinstallieren Sie zunächst die Advanced Edition vom Server und installieren Sie dann die Standard Edition-ISO-Imagedatei vom Identity Manager-Medium.

Folgende Funktionen stehen in Identity Manager Standard Edition nicht zur Verfügung:

- Der Rollenzuordnungsadministrator ist nicht verfügbar.
- Folgende Beschränkungen gelten für die Benutzeranwendung:
  - **Geschäftsbenutzer haben nur Zugriff auf die Registerkarte „Identitätsselbstbedienung“:** Wenn Sie sich als Geschäftsbenutzer bei der Standard Edition von Identity Manager anmelden, wird in der Benutzeranwendung nur die Registerkarte *Identitätsselbstbedienung* angezeigt. Wenn Sie sich als Benutzeranwendungsadministrator anmelden, steht zudem die Registerkarte *Administration* zur Verfügung.
  - **Rollen und Ressourcen werden nicht unterstützt:** Die Verwendung von Rollen und Ressourcen ist nur in der Advanced Edition möglich. In der Standard Edition ist die Registerkarte *Rollen und Ressourcen* nicht verfügbar.
  - **Die Registerkarte „Konformität“ wird nicht unterstützt:** Die Registerkarte *Konformität* steht nur in Identity Manager 4.0.1 Advanced Edition zur Verfügung. In der Standard Edition ist die Registerkarte *Konformität* nicht verfügbar.
  - **Das Arbeits-Dashboard ist nicht verfügbar:** In der Standard Edition steht die Registerkarte *Arbeits-Dashboard* nicht zur Verfügung.
  - **Benutzerdefinierte Rollen werden nicht unterstützt:** Die Definition von benutzerdefinierten Rollen ist nicht möglich. Die Standard Edition unterstützt nur die Verwendung von Systemrollen.
  - **Workflows werden nicht unterstützt:** Das Initiieren von Genehmigungs-Workflows ist nicht möglich.
  - **REST-APIs:** REST-APIs bezüglich Rollen, Ressourcen, Workflows usw. sind nicht verfügbar.
  - **Vereinfachtes Sicherheitsmodell:** Die Standard Edition bietet ein vereinfachtes Sicherheitsmodell, mit dem die unbeabsichtigte Verwendung von Funktionen der Advanced Edition verhindert wird. Sie müssen nur die folgenden Administratorrollen zuweisen:
    - **Benutzeranwendungsadministrator:** Ein Benutzeranwendungsadministrator ist berechtigt, alle Verwaltungsfunktionen in Verbindung mit der Identity Manager-Benutzeranwendung auszuführen. Dies umfasst den Zugriff auf die Registerkarte *Administration* der Benutzeroberfläche von Identity Manager, um die dort verfügbaren Verwaltungsaktionen auszuführen.
    - **Berichtsadministrator:** Dieser Benutzer kann alle Funktionen in der Berichterstellungsdomäne verwenden. Der Berichtsadministrator kann für alle Objekte alle Aktionen innerhalb der Berichterstellungsdomäne durchführen.
    - **Sicherheitsadministrator:** Diese Rolle bietet Mitgliedern die ganze Funktionspalette innerhalb der Sicherheitsdomäne. Der Sicherheitsadministrator kann für alle Objekte alle möglichen Aktionen innerhalb der Sicherheitsdomäne

durchführen. Da diese Rolle berechtigt ist, Benutzerzugriffe für alle Funktionen von Identity Manager Advanced Edition zu erteilen bzw. zu delegieren, wird sie von den Rollen Benutzeranwendungsverwaltung und Berichtsverwaltung getrennt behandelt.

Hinweis: Novell hat zu Testzwecken das Sicherheitsmodell in der Standard Edition nicht gesperrt. Der Sicherheitsadministrator kann daher alle Domänenadministratoren und beauftragte Administratoren sowie andere Sicherheitsadministratoren zuweisen. In der Produktionsumgebung werden diese erweiterten Funktionen jedoch nicht unterstützt, wie in der Endbenutzer-Lizenzvereinbarung beschrieben. In Produktionsumgebungen wird die Zuweisung der Administratoren durch die Lizenzierung beschränkt. Novell sammelt Überwachungsdaten in der Audit-Datenbank, um sicherzustellen, dass die Lizenzierung in der Produktionsumgebung eingehalten wird. Darüber hinaus ist es empfehlenswert, die Sicherheitsadministratorberechtigung nur einem Benutzer zu erteilen.

Weitere Informationen zu den Funktionen der Benutzeranwendung finden Sie im *Rollenbasiertes Bereitstellungsmodul für Identity Manager 4.0 Benutzeranwendung: Administrationshandbuch*.

- Folgende Beschränkungen gelten für das Identitätsberichterstellungsmodul:
  - **Treiber „Verwaltetes System - Gateway“ ist deaktiviert:** Der Treiber „Verwaltetes System - Gateway“ kann von jedem verwalteten System, das Berechtigungen unterstützt und in Identity Manager 4.0.1 für die Datenerfassung aktiviert wurde, Informationen abrufen.

    Der Treiber „Verwaltetes System - Gateway“ ist in der Standard Edition von Identity Manager deaktiviert.
  - **Berichte enthalten nur Identitätsdepotinformationen:** Berichte, die mit Identity Manager Standard Edition generiert werden, enthalten nur Identitätsdepotdaten und keine Informationen zu verbundenen verwalteten Systemen.
  - **Berichte enthalten keine Verlaufsdaten:** In der Standard Edition ist es beim Erstellen von Berichten nicht möglich, Daten zum Statusverlauf abzurufen. Die Standard Edition gibt nur Daten wieder, die den aktuellen Status des Systems widerspiegeln.
  - **Einige Berichte sind nicht verfügbar:** In Identity Manager 4.0 und 4.0.1 wurden mehrere neue Berichte eingefügt. Die Standard Edition umfasst keine Berichte für verbundene Systeme sowie Berichte mit Verlaufsdaten.
  - **Einige Berichte enthalten keine Daten:** Einige Berichte sind nur für die Verwendung mit der Identity Manager Advanced Edition sinnvoll, da sie Daten beinhalten, die in der Standard Edition nicht verfügbar sind, z. B. Rollen, Ressourcen und Workflow-Prozesse.

3.3 Compliance Management-Plattform

Die Novell Compliance Management-Plattform kombiniert die Novell-Produkte zur Identitäts-, Zugriffs- und Sicherheitsverwaltung mit bewährten Werkzeugen, die eine einfache Implementierung und Verwaltung der Lösung ermöglichen. Die Plattform integriert Identitäts- und Zugriffsdaten in Sicherheitsdaten- und Ereignismanagement-Technologien und liefert so einen holistischen Echtzeitüberblick über alle Netzwerkereignisse im Unternehmen. Diese enge Integration liefert leistungsstarke Funktionen für das Risikomanagement und stellt sicher, dass die Geschäftspolitik automatisch in den IT-Alltag eingebunden wird. Weitere Informationen hierzu finden Sie auf der Website zur Compliance Management-Plattform (http://www.novell.com/documentation/ncmp10/).

3.4 Aktivieren der Standard und Advanced Edition von Identity Manager

Identity Manager Advanced Edition und Standard Edition müssen innerhalb von 90 Tagen nach der Installation aktiviert werden, anderenfalls wird ihre Funktion eingestellt. Die ISO-Imagedateien für Identity Manager Advanced Edition und Standard Edition funktionieren bis zu 90 Tage. Sie können Identity Manager-Produkte zu einem beliebigen Zeitpunkt während oder nach Ablauf der 90 Tage aktivieren. Weitere Informationen hierzu finden Sie unter „Activating Novell Identity Manager Products“ (Aktivieren von Novell Identity Manager-Produkten) im *Identity Manager 4.0.1 Framework Installation Guide* (Installationshandbuch zu Identity Manager 4.0.1 Framework).

Wenn die Aktivierung der Standard Edition auf ein vorhandenes, nicht aktiviertes Advanced Edition-System angewendet wird, funktionieren der Metaverzeichnis-Server und die Treiber nicht mehr.

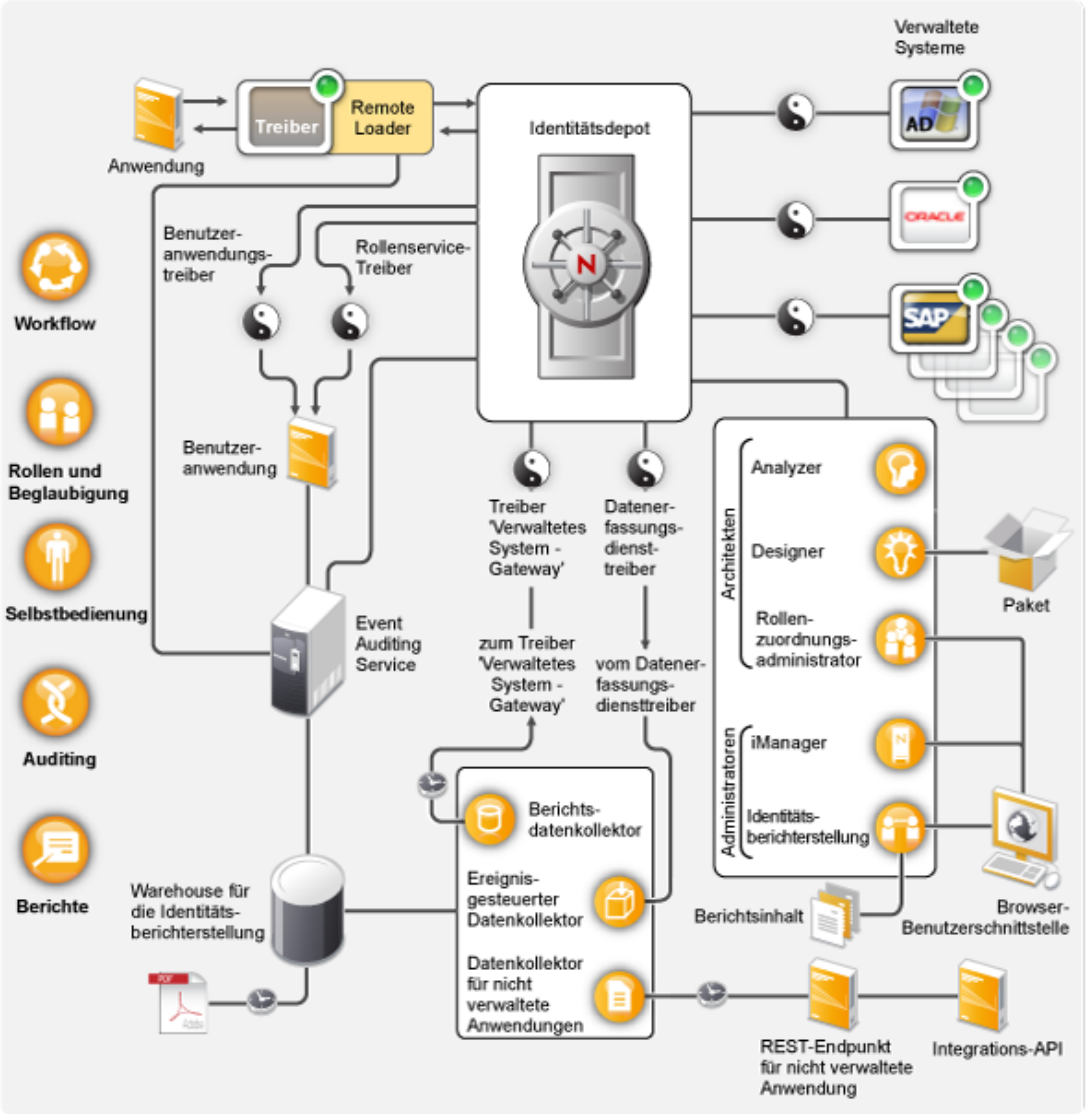
Hinweis: Wenn Sie sowohl Identity Manager Advanced Edition als auch Identity Manager Standard Edition verwenden, stellen Sie sicher, dass Sie die korrekte Aktivierung auf dem entsprechenden Server durchführen.

Identity Manager-Architektur

4

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 7 vorgestellt wurden: Datensynchronisierung, Workflow, Rollen, Beglaubigung, Selbstbedienung und Revision/Berichterstellung.

Abbildung 4-1 *High-Level-Architektur von Identity Manager*



Die einzelnen Komponenten werden in den folgenden Abschnitten erläutert:

- Abschnitt 4.1, „Datensynchronisierung“, auf Seite 28
- Abschnitt 4.2, „Workflow, Rollen, Beglaubigung und Selbstbedienung“, auf Seite 33
- Abschnitt 4.3, „Revision und Berichterstellung“, auf Seite 36

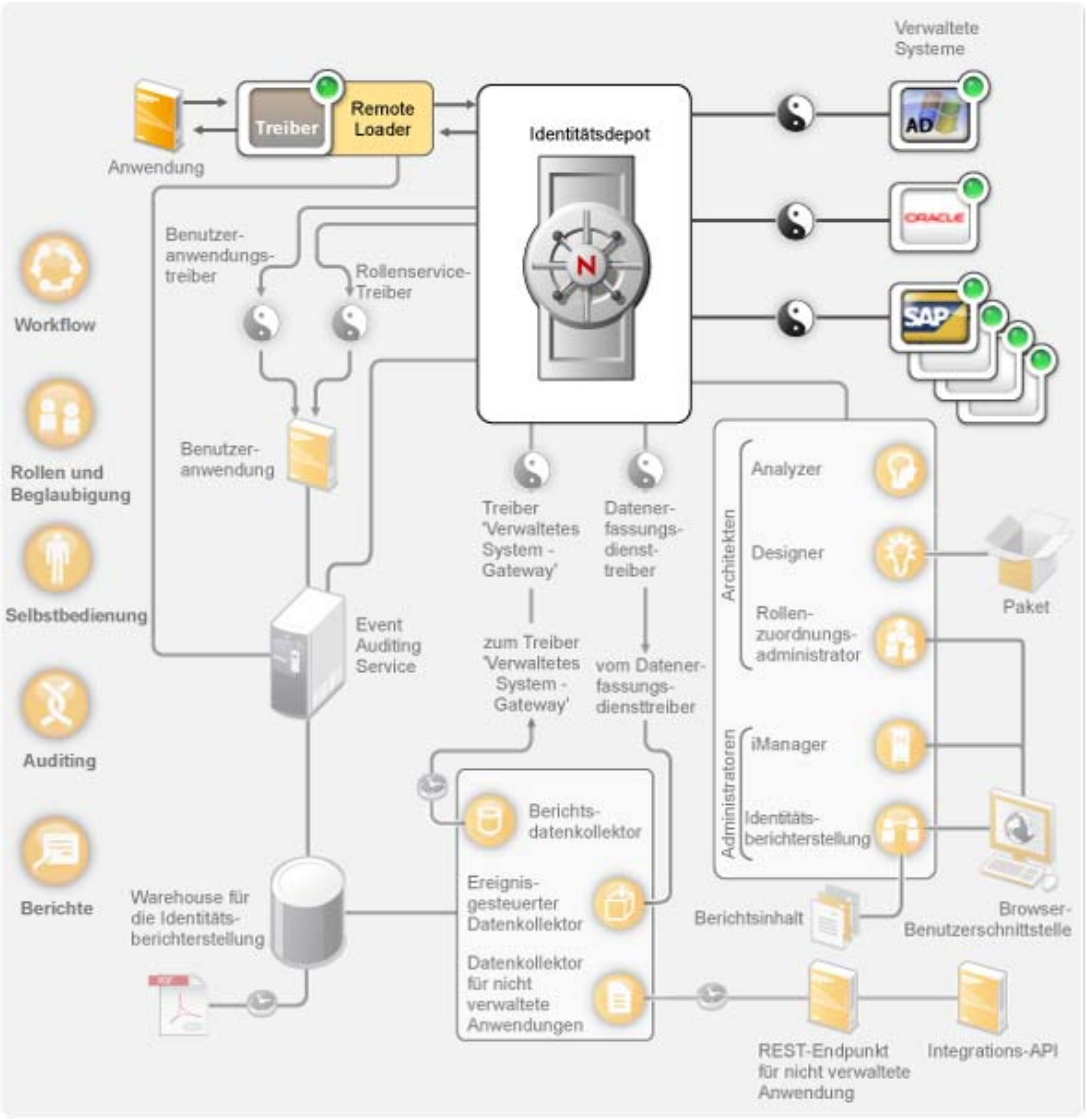
4.1 Datensynchronisierung

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 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 Identity Manager-Engine, die Treiber, der Remote Loader und die verbundenen Anwendungen. Diese Komponenten sind im folgenden Diagramm abgebildet.

Abbildung 4-2 *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 4.1.1, „Komponenten“, auf Seite 29
- Abschnitt 4.1.2, „Wichtige Konzepte“, auf Seite 30

4.1.1 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.

Identity Manager-Engine: Wenn im Identitätsdepot oder in einer verbundenen Anwendung Daten geändert werden, verarbeitet die Identity Manager-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 Identity Manager-Engine wird auch als Metaverzeichnis-Engine bezeichnet.

Treiber: Treiber stellen eine Verbindung zu den Anwendungen her, deren Identitätsinformationen Sie verwalten möchten. Ein Treiber hat zwei grundlegende Aufgaben: das Melden von Datenänderungen (Ereignissen) in der Anwendung an die Identity Manager-Engine sowie das Ausführen von Datenänderungen (Befehlen), die von der Identity Manager-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 Identity Manager-Engine befindet, müssen Sie lediglich den Treiber auf diesem Server installieren. Befindet sich die Anwendung jedoch nicht auf demselben Server wie die Identity Manager-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 Identity Manager-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.

4.1.2 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 Identity Manager-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 Identity Manager-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 Identity Manager-Engine den Benutzer mithilfe der 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.

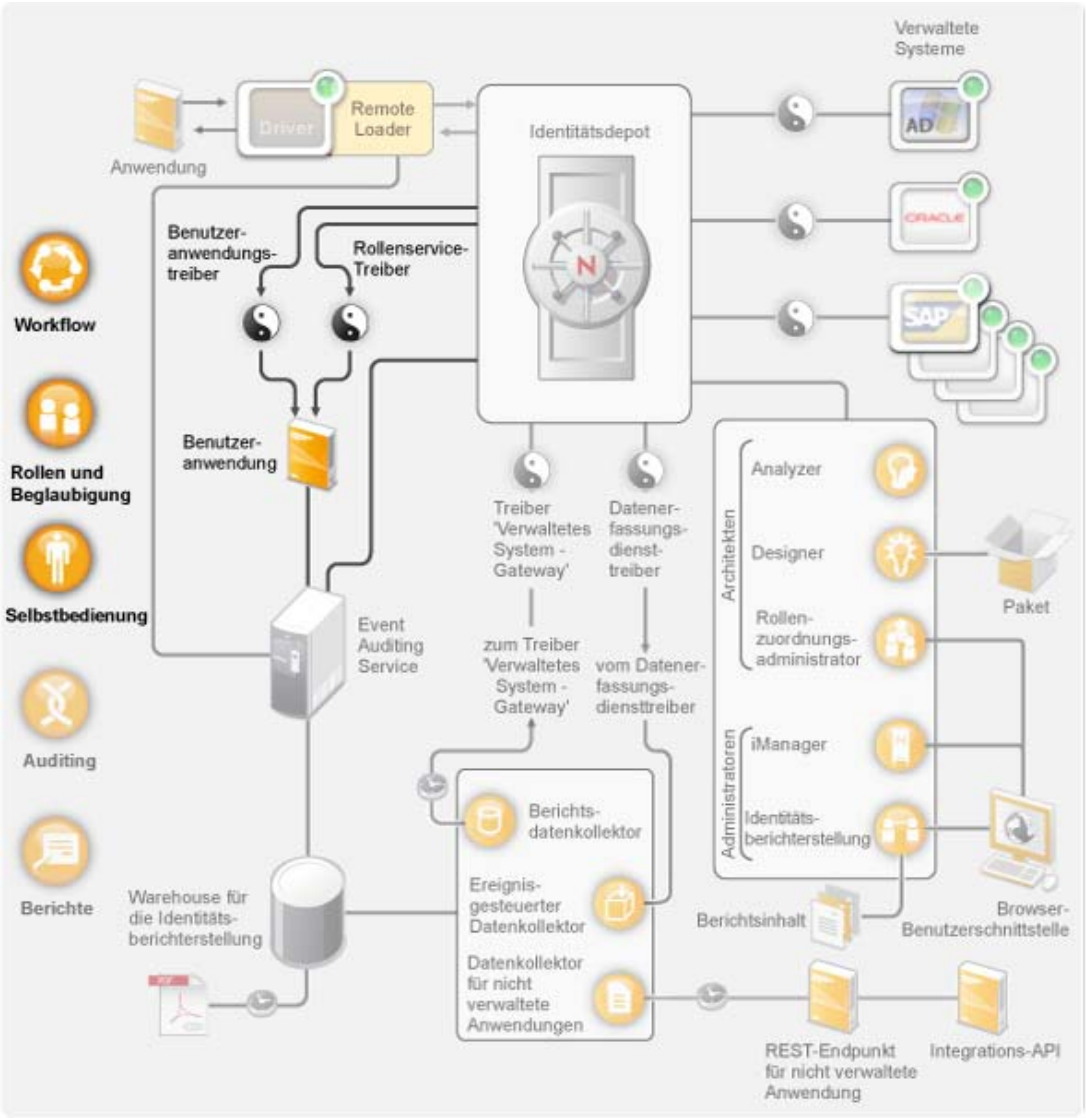
4.2 Workflow, Rollen, Beglaubigung und Selbstbedienung

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 eine Komponente von Identity Manager 4.0.1 Advanced Edition. Mit dem rollenbasierten Bereitstellungsmodul stehen Ihnen neben den Funktionen der Standard-Benutzeranwendung die erweiterte Selbstbedienung, der Genehmigungsworkflow, die rollenbasierte Bereitstellung, Funktionstrennungsbeschränkungen und die Beglaubigung zur Verfügung. Identity Manager 4.0.1 Advanced Edition umfasst die Standardfunktionen und die Funktionen des rollenbasierten Bereitstellungsmoduls.

Abbildung 4-3 *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 4.2.1, „Komponenten“, auf Seite 34
- Abschnitt 4.2.2, „Wichtige Konzepte“, auf Seite 35

4.2.1 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.

Rollen- und Ressourcenservice-Treiber: Der Rollen- und Ressourcenservice-Treiber verwaltet alle Rollen- und Ressourcenzuweisungen, startet Workflows für Rollen- und Ressourcenzuweisungsanforderungen, 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.

4.2.2 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 Systemfunktionen 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.

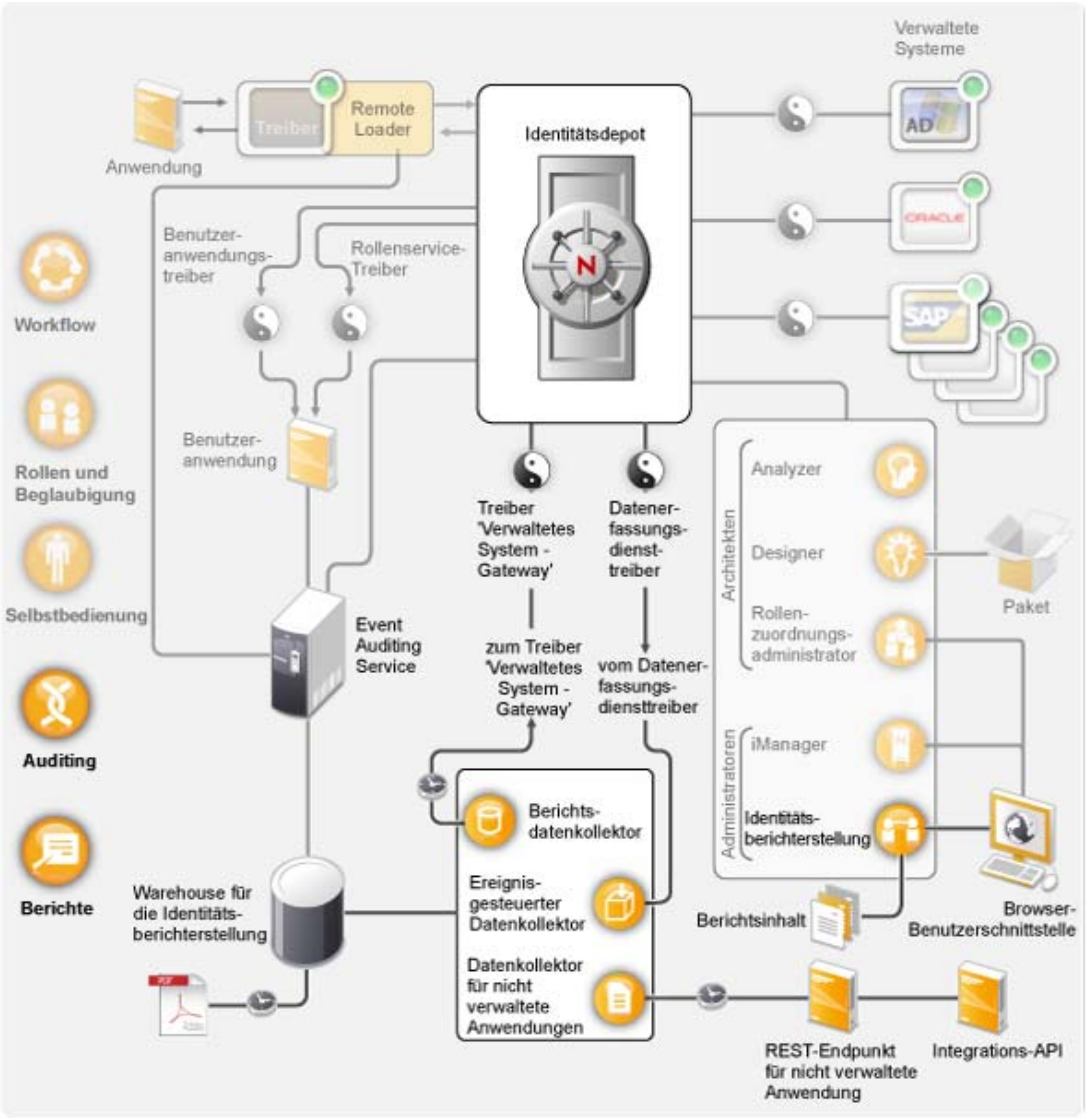
Der Rollenmanager kann dieselben Aufgaben durchführen wie der Rollenmodul-Administrator, mit Ausnahme des Verwaltens von Funktionstrennungsbeschränkungen, der Konfiguration des Rollensystems und des Ausführens aller Berichte. Außerdem bestehen für den Rollenmodul-Administrator keine Bereichsbeschränkungen 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.

4.3 Revision und Berichterstellung

Revision und Berichterstellung stehen über das Identitätsberichterstellungsmodul, eine neue Funktion von Identity Manager 4.0.1, zur Verfügung (siehe nachfolgendes Diagramm).

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



Mit dem Identitätsberichterstellungsmodul können Sie Berichte generieren, die unternehmenskritische Informationen zu verschiedenen Aspekten Ihrer Identity Manager-Konfiguration liefern, einschließlich erfasster Informationen zu Identitätsdepots oder verwalteten Systemen, z. B. Active Directory oder SAP. Das Identitätsberichterstellungsmodul verwaltet die Daten mittels folgender Komponenten:

Event Auditing Service: Dieser Dienst protokolliert Aktionen, die im Berichterstellungsmodul durchgeführt wurden, z. B. das Importieren, Ändern, Löschen oder Planen eines Berichts. Der Event Auditing Service (EAS) protokolliert Aktionen, die im rollenbasierten Bereitstellungsmodul und im Rollenzuordnungsadministrator durchgeführt wurden.

Identitätsinformations-Warehouse: Repository für folgende Informationen:

- Berichtverwaltungsinformationen, z. B. Berichtsdefinitionen, Berichtzeitpläne und abgeschlossene Berichte, für die Berichterstellung verwendete Datenbankansichten und Konfigurationsinformationen.

- Identifikationsdaten, die vom Berichtsdatenkollektor, vom ereignisgesteuerten Datenkollektor und vom Datenkollektor für nicht verwaltete Anwendungen gesammelt wurden.
- Revisionsdaten mit Ereignissen, die vom Event Auditing Service erfasst wurden.

Die Daten des Identitätsinformations-Warehouses werden in der SIEM-Datenbank (Security Information and Event Management) gespeichert.

Datenerfassungsdienst: Ein Dienst, der Informationen von verschiedenen Quellen innerhalb der Organisation sammelt. Der Datenerfassungsdienst ist in drei Unterdienste unterteilt:

- **Berichtsdatenkollektor:** Verwendet ein Pull-Modell zum Abrufen von Daten aus einer oder mehreren Identitätsdepot-Datenquellen. Die Sammlung der Daten wird regelmäßig auf Grundlage der festgelegten Konfigurationsparameter durchgeführt. Der Kollektor ruft zum Abrufen der Daten den Treiber „Verwaltetes System - Gateway“ auf.
- **Ereignisgesteuerter Datenkollektor:** Verwendet ein Push-Modell zum Sammeln von Ereignisdaten, die vom Datenerfassungsdiensttreiber erfasst wurden.
- **Datenkollektor für nicht verwaltete Anwendungen:** Ruft Daten von einer oder mehreren nicht verwalteten Anwendungen ab, indem er einen speziell für jede Anwendung geschriebenen REST-Endpunkt aufruft. Nicht verwaltete Anwendungen sind Anwendungen in Ihrem Unternehmen, die nicht mit dem Identitätsdepot verbunden sind. Weitere Informationen hierzu finden Sie unter „REST Services for Reporting“ (REST-Dienste für Berichterstellung) im *Identity Reporting Module Guide* (Handbuch zum Identitätsberichterstellungsmodul).

Datenerfassungsdiensttreiber: Ein Treiber, der Änderungen an Objekten im Identitätsdepot erfasst, z. B. Konten, Rollen, Ressourcen, Gruppen und Teammitgliedschaften. Der Datenerfassungsdiensttreiber registriert sich beim Datenerfassungsdienst und gibt Änderungsereignisse (z. B. Datensynchronisierung sowie Hinzufügen, Ändern und Löschen von Ereignissen) an den Datenerfassungsdienst weiter.

Änderungen an folgenden Objekten werden aufgezeichnet:

- Benutzerkonten und Identitäten
- Rollen und Rollenebenen
- Gruppen

  Hinweis: Dynamische Gruppen werden vom Berichterstellungsmodul nicht unterstützt. Es werden nur Berichte von statischen Gruppen generiert.

- Gruppenmitgliedschaften
- Bereitstellungsanforderungsdefinitionen
- Funktionstrennungsdefinitionen und -verletzungen
- Benutzerberechtigungsverknüpfungen
- Ressourcendefinitionen und Ressourcenparameter
- Rollen- und Ressourcenzuweisungen
- Identitätsdepotberechtigungen, Berechtigungstypen und Treiber

Treiber „Verwaltetes System - Gateway“ Dieser Treiber sammelt Daten von verwalteten Systemen. Der Treiber führt zum Abrufen der Daten der verwalteten Systeme eine Identitätsdepotabfrage durch. Folgende Daten werden abgerufen:

- Liste aller verwalteten Systeme

- Liste mit allen Konten für die verwalteten Systeme
- Berechtigungstypen, Werte und Zuweisungen sowie Benutzerkontenprofile für die verwalteten Systeme

Identitätsberichterstellung: Über die Benutzeroberfläche des Berichterstellungsmoduls können Sie problemlos festlegen, dass die Berichtgenerierung außerhalb der Hauptgeschäftszeit ausgeführt und somit die Systemleistung nicht beeinträchtigt wird. Weitere Informationen hierzu finden Sie im *Identity Reporting Module Guide* (Handbuch zum Identitätsberichterstellungsmodul).

Berichte: Identity Manager enthält vordefinierte Berichte, um die Daten im Identitätsinformations-Warehouse sinnvoll darzustellen. Sie können auch benutzerdefinierte Berichte erstellen. Weitere Informationen zu den Berichten finden Sie unter *Verwenden von Identity Manager 4.0 Berichten*. Weitere Informationen zu benutzerdefinierten Berichten finden Sie unter „Creating Custom Report Definitions“ (Erstellen von benutzerdefinierten Berichtsdefinitionen) im *Identity Reporting Module Guide* (Handbuch zum Identitätsberichterstellungsmodul).

REST-Endpunkt für nicht verwaltete Anwendung: Eine nicht verwaltete Anwendung ist eine Anwendung, die nicht mit dem Identitätsdepot verbunden ist, jedoch Daten enthält, die im Bericht aufgezeichnet werden sollen. Wenn Sie einen REST-Endpunkt für die Anwendung festlegen, kann das Berichterstellungsmodul Daten aus der Anwendung abrufen.

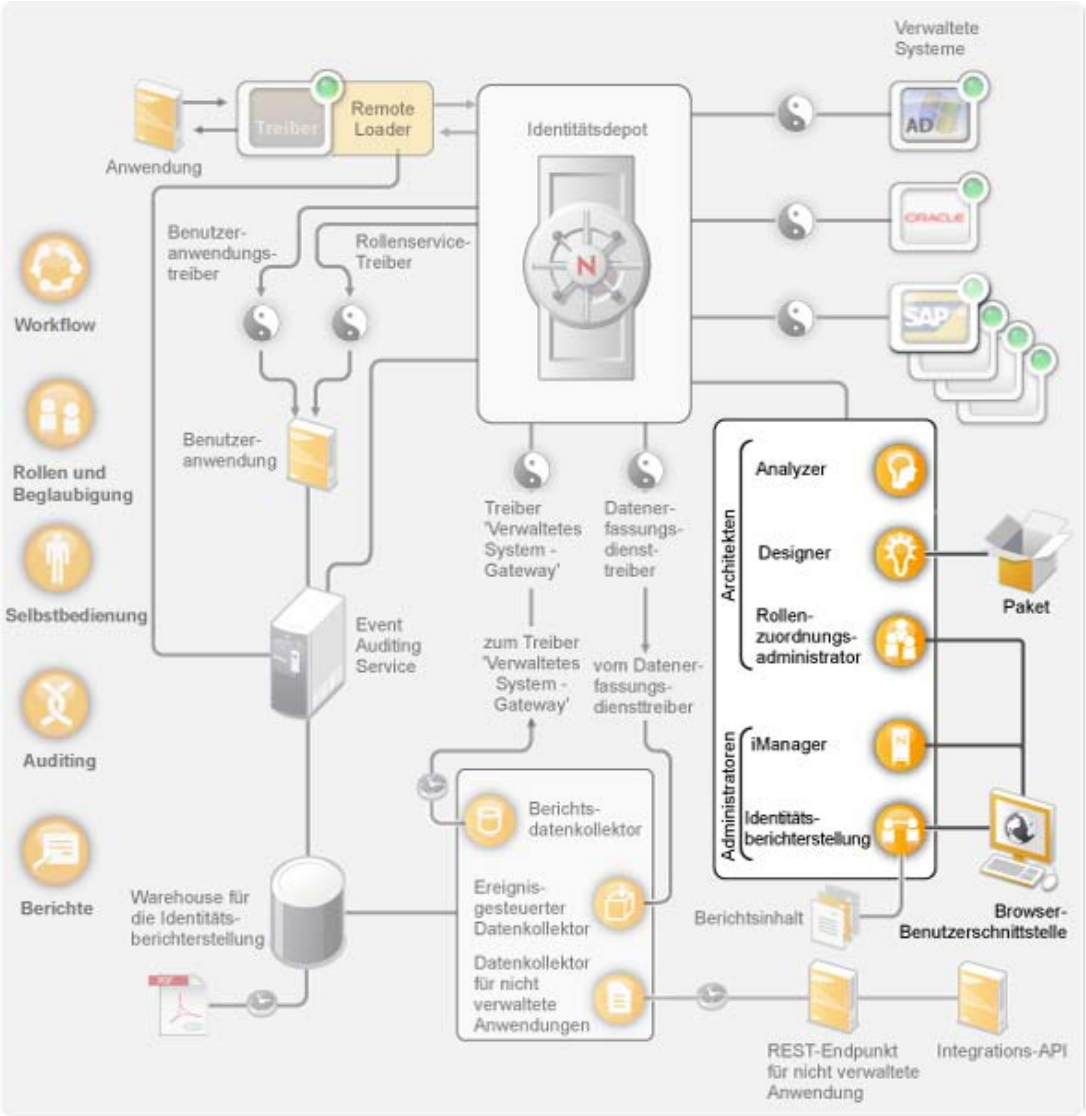
Integrations-API: Das Identitätsberichterstellungsmodul bietet mehrere REST-APIs, mit denen Sie REST-Endpunkte für nicht verwaltete Anwendungen festlegen sowie benutzerdefinierte Anwendungen für die Berichterstellung schreiben können.

Identity Manager-Werkzeuge

5

Identity Manager stellt Ihnen Werkzeuge zum Erstellen und Verwalten Ihrer Identity Manager-Lösung zur Verfügung. Mit jedem Werkzeug werden spezifische Funktionen ausgeführt.

Abbildung 5-1 *Identity Manager-Werkzeuge*



Mithilfe von Designer können Sie Ihr Identity Manager-System in einer Offline-Umgebung entwerfen, erstellen und konfigurieren und Ihre Änderungen dann in Ihr Live-System übertragen. Darüber hinaus bietet Designer Paketverwaltungsfunktionen zum Vorkonfigurieren und Anpassen der Identity Manager-Treiberrichtlinien. Analyzer wird beim Erstellen der Identity Manager-Lösung zur Datenanalyse und -bereinigung sowie zur Vorbereitung der Datensynchronisierung verwendet.

Der Rollenzuordnungsadministrator dient zum Erstellen und Verwalten von Rollen in Ihrer Identity Manager-Lösung.

Mit iManager können Sie die gleichen Aufgaben wie mit Designer durchführen und zudem den Zustand Ihres Systems überwachen. Die Paketverwaltung wird in iManager jedoch nicht unterstützt. Es ist empfehlenswert, iManager für Verwaltungsaufgaben und Designer für Konfigurationsaufgaben, die Änderungen an Paketen, Modellierung und Tests vor der Bereitstellung erfordern, zu verwenden.

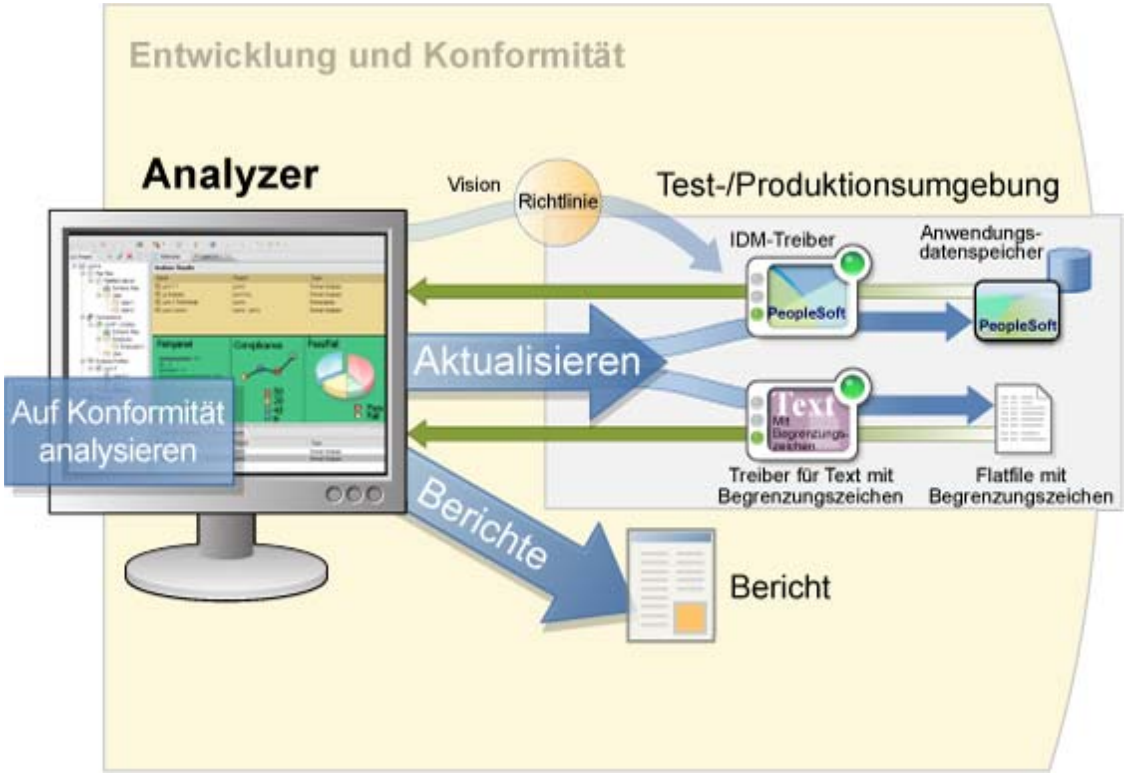
In den folgenden Abschnitten finden Sie weitere Informationen zu den einzelnen Werkzeugen:

- Abschnitt 5.1, „Analyzer“, auf Seite 42
- Abschnitt 5.2, „Designer“, auf Seite 43
- Abschnitt 5.3, „iManager“, auf Seite 44
- Abschnitt 5.4, „Rollenzuordnungsadministrator“, auf Seite 44
- Abschnitt 5.5, „Identitätsberichterstellung“, auf Seite 45

5.1 Analyzer

Analyzer ist ein Eclipse-basierter Satz von Identitätsverwaltungswerkzeugen, der Ihnen hilft, sicherzustellen, dass mithilfe der Datenanalyse und Datenbereinigung sowie des Datenabgleichs, der Datenüberwachung und der Datenberichterstellung interne Datenqualitätsrichtlinien eingehalten werden. Mit Analyzer können Sie alle Datenspeicher des Unternehmens analysieren, verbessern und kontrollieren.

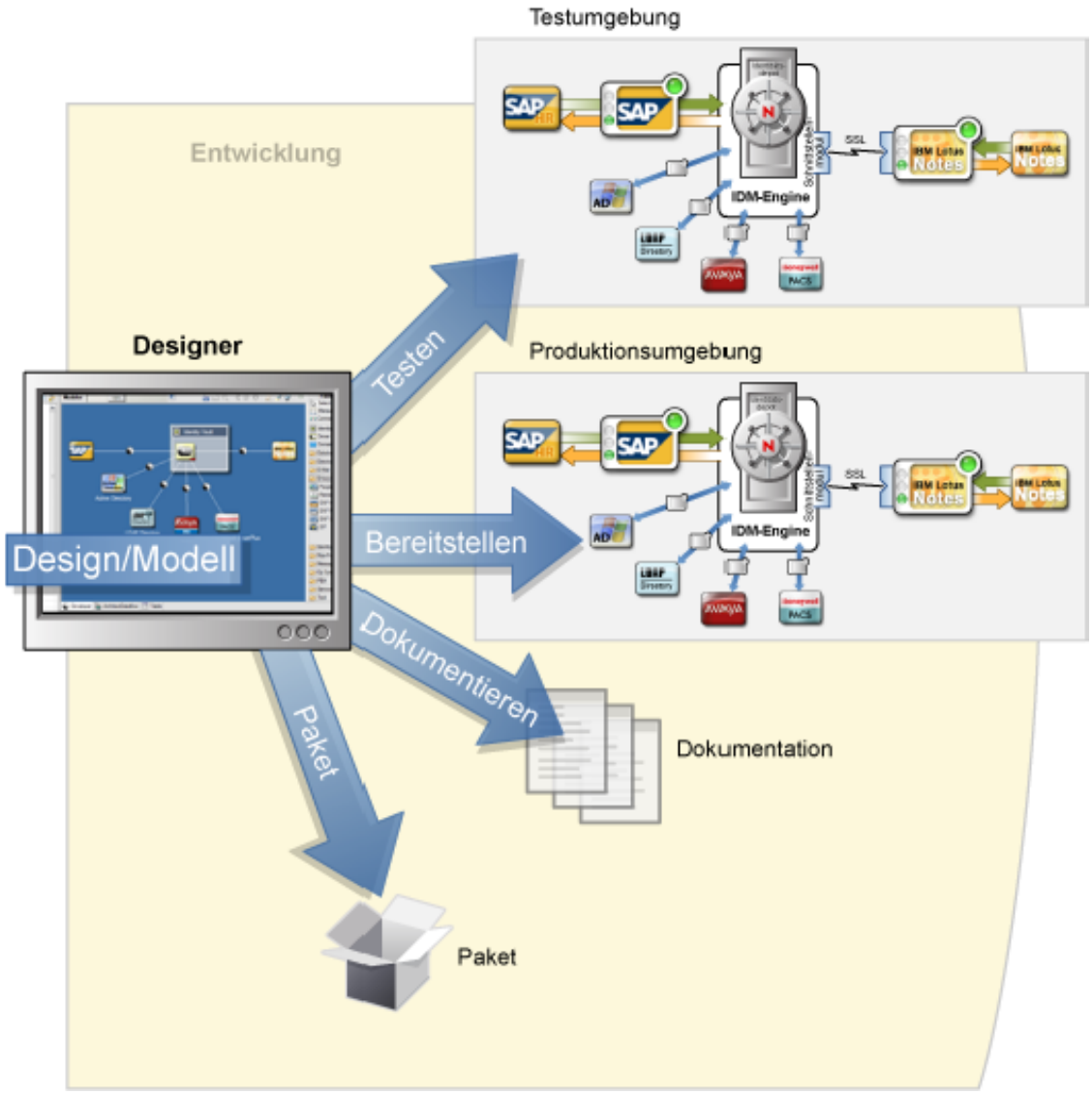
Abbildung 5-2 *Analyzer für Identity Manager*



5.2 Designer

Designer ist ein Eclipse-basiertes Werkzeug, mit dessen Hilfe Sie das Identity Manager-System entwerfen, bereitstellen und dokumentieren können. 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 5-3 *Designer für Identity Manager*



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.

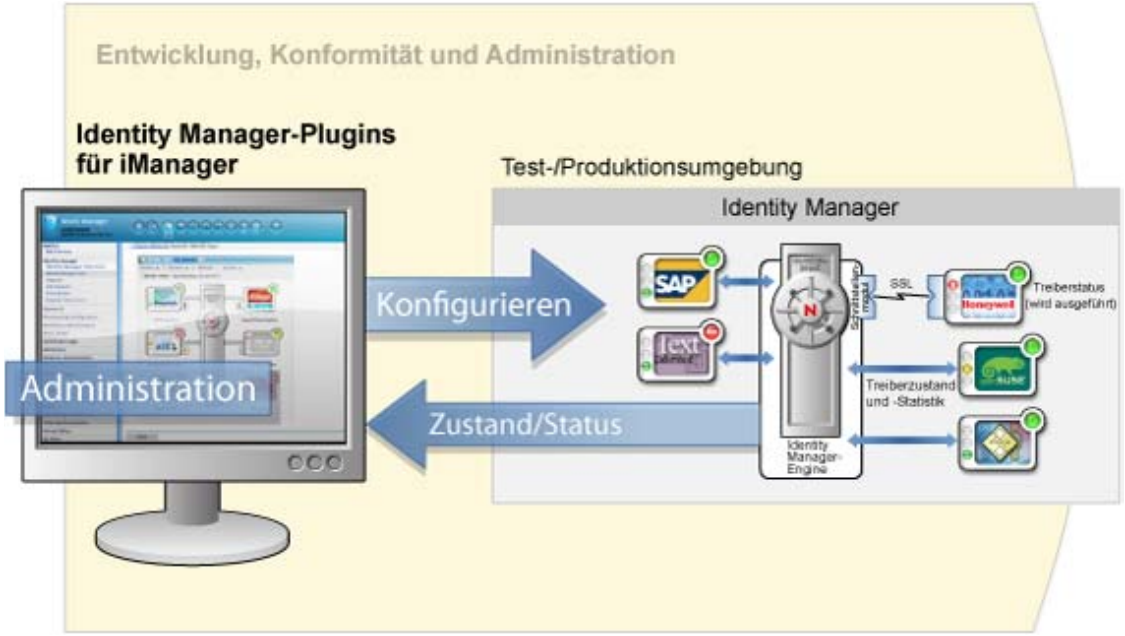
Bereitstellen: Ihre in Designer ausgeführte Arbeit wird erst dann in Ihrer Produktionsumgebung bereitgestellt, wenn Sie die Bereitstellung initiieren. Dadurch besitzen Sie die Freiheit, zu experimentieren, die Ergebnisse zu testen und Probleme zu beheben, bevor das System in Ihrer Produktionsumgebung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

5.3 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.

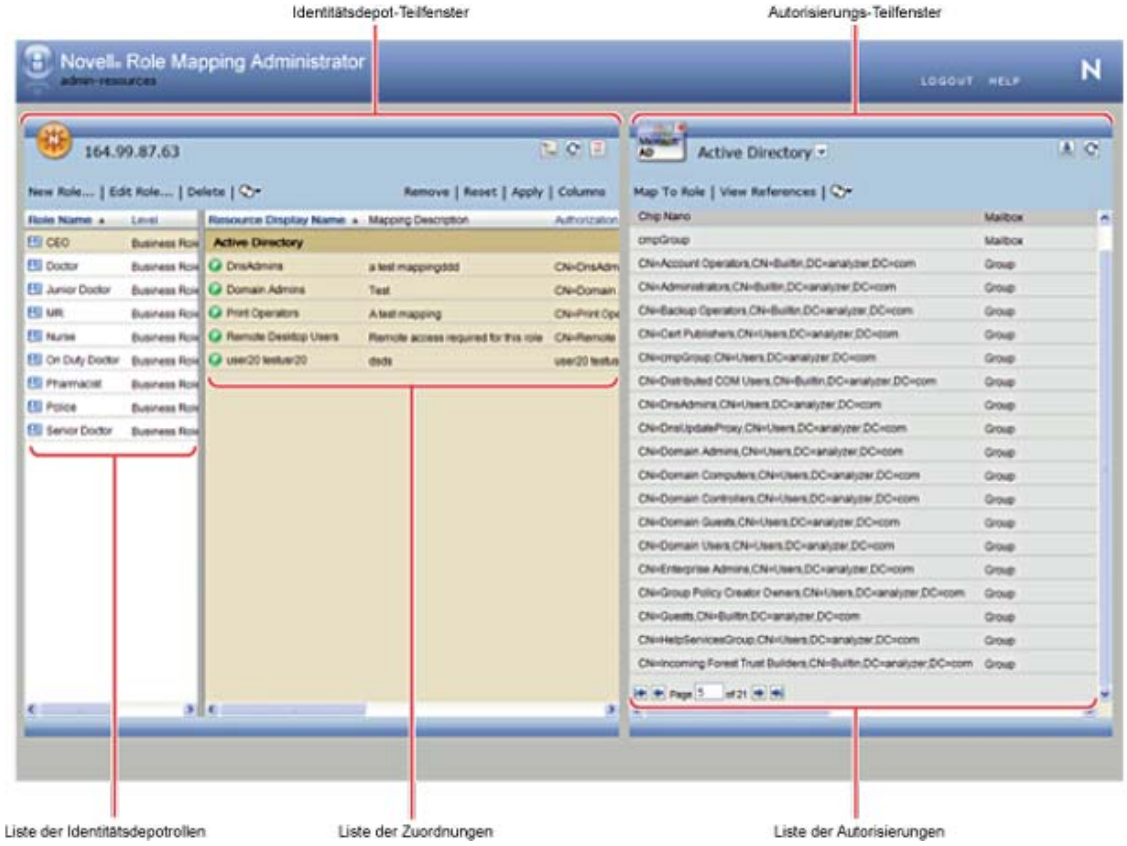
Abbildung 5-4 *Novell iManager*



5.4 Rollenzuordnungsadministrator

Der Rollenzuordnungsadministrator ist ein Webservice, der die Autorisierungen und Berechtigungen ermittelt, die innerhalb Ihres Haupt-IT-Systems erteilt werden können. Er ermöglicht es Geschäftsanalysten, nicht nur IT-Administratoren, bestimmte Autorisierungen für bestimmte Geschäftsrollen zu definieren und zu verwalten.

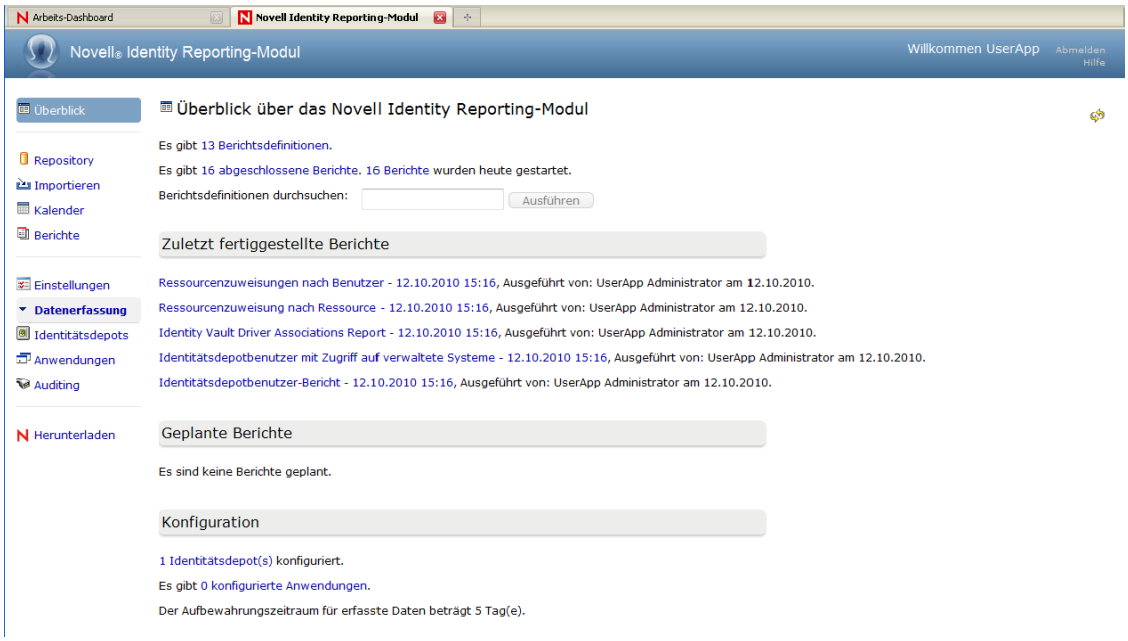
Abbildung 5-5 *Rollenzuordnungsadministrator*



5.5 Identitätsberichterstellung

Mit dem Identitätsberichterstellungsmodul können Sie Berichte generieren, die unternehmenskritische Informationen zu verschiedenen Aspekten Ihrer Identity Manager-Konfiguration liefern, einschließlich erfasster Informationen zu Identitätsdepots oder verwalteten Systemen, z. B. Active Directory oder SAP. Das Berichterstellungsmodul enthält eine Reihe von vordefinierten Berichtsdefinitionen, die Sie zum Generieren von Berichten verwenden können. Zusätzlich haben Sie die Möglichkeit, benutzerdefinierte Berichte zu importieren, die in einem Drittanbieter-Werkzeug definiert sind. Über die Benutzeroberfläche des Berichterstellungsmoduls können Sie problemlos festlegen, dass die Berichtgenerierung außerhalb der Hauptgeschäftszeit ausgeführt und somit die Systemleistung nicht beeinträchtigt wird.

Abbildung 5-6 *Identitätsberichterstellungsmodul*



Das Berichterstellungsmodul bietet mehrere offene Integrationspunkte. Wenn Sie beispielsweise Daten über Anwendungen von Drittanbietern erfassen möchten, die nicht mit Identity Manager verbunden sind, können Sie einen benutzerdefinierten REST-Endpunkt implementieren, um Daten von diesen Anwendungen zu erfassen. Darüber hinaus können Sie die Daten anpassen, die per Push-Verfahren in das Identitätsdepot übertragen werden. Wenn diese Daten verfügbar sind, können Sie benutzerdefinierte Berichte schreiben, um diese Informationen anzuzeigen.

Weitere Schritte

6

Wenn Sie die Komponenten verstanden haben, aus denen Identity Manager 4.0.1 besteht, verwenden Sie im nächsten Schritt die Dokumentation, um Ihre eigene Identity Manager-Lösung zu erstellen. In den folgenden Abschnitten wird erläutert, wo die Dokumentation für die aufgeführten Aufgaben zu finden ist:

6.1 Planen einer Identity Manager-Lösung

Der erste Schritt beim Entwerfen einer Identity Manager-Lösung besteht darin zu entscheiden, was genau die Aufgabe der Lösung in Ihrem Unternehmen sein soll. Lesen Sie den Abschnitt „Planning“ (Planung) im *Identity Manager 4.0.1 Framework Installation Guide* (Installationshandbuch zu Identity Manager 4.0.1 Framework), um einen Plan für Ihre Identity Manager-Lösung mithilfe von Designer zu entwerfen. Sie können auch eine Benutzeranwendungs-Lösung erstellen. Verwenden Sie hierzu das *Benutzeranwendung: Designhandbuch*.

Mit Designer können Sie Informationen in einem Projekt erfassen und die Informationen für andere Personen freigeben. Sie können die Lösung im Designer zunächst modellieren, bevor Sie Änderungen vornehmen. Weitere Informationen über Designer finden Sie unter *Designer für Identity Manager*.

6.2 Vorbereiten der Daten für die Synchronisierung

Wenn Sie Ihren Plan erstellt haben, müssen Sie die Daten in Ihrer Umgebung für die Synchronisierung vorbereiten. Mithilfe von Analyzer analysieren und bereinigen Sie die Daten und bereiten diese für die Synchronisierung vor. Weitere Informationen hierzu finden Sie im *Analyzer 4.0.1 for Identity Manager Administration Guide* (Administrationshandbuch zu Analyzer 4.0.1 für Identity Manager).

6.3 Installation oder Aufrüstung von Identity Manager

Wenn Sie Ihren Plan erstellt und die Daten vorbereitet haben, können Sie Identity Manager installieren. Wenn Sie eine kleine bis mittlere IT-Umgebung haben und Identity Manager zum ersten Mal verwenden, ist es am besten, das integrierte Installationsprogramm zu verwenden. Das integrierte Installationsprogramm installiert und konfiguriert alle in Identity Manager enthaltenen Komponenten. Weitere Informationen finden Sie im *Identity Manager 4.0.1 Integrated Installation Guide* (Handbuch zur integrierten Installation von Identity Manager 4.0).

Wenn Sie bereits über ein Identity Manager-System verfügen oder eine große IT-Umgebung haben, ziehen Sie das *Identity Manager 4.0.1 Framework Installationshandbuch* zu Rate, um die verschiedenen Identity Manager-Komponenten zu installieren bzw. aufzurüsten. Jede Identity Manager-Komponente wird separat installiert und konfiguriert, sodass Sie Ihre Identity Manager-Lösung an Ihre Anforderungen anpassen können.

- Installationsanweisungen finden Sie unter „Installation“ im *Identity Manager 4.0.1 Framework Installationshandbuch*.
- Aufrüstungsanweisungen finden Sie unter „Performing an Upgrade“ (Durchführen einer Aufrüstung) im *Identity Manager 4.0.1 Upgrade and Migration Guide* (Aufrüstungs- und Migrationshandbuch zu Identity Manager 4.0.1).
- Wenn Sie ein vorhandenes System auf neue Hardware migrieren, lesen Sie „Performing an Upgrade“ (Durchführen einer Aufrüstung) im *Identity Manager 4.0.1 Upgrade and Migration Guide* (Aufrüstungs- und Migrationshandbuch zu Identity Manager 4.0.1).
- Informationen zur Migration des rollenbasierten Bereitstellungsmoduls finden Sie im *Rollenbasierten Bereitstellungsmodul für Novell Identity Manager 4.0 Benutzeranwendung: Migrationshandbuch*.

6.4 Konfigurieren von Identity Manager

Nach der Installation von Identity Manager müssen Sie verschiedene Komponenten konfigurieren, damit Sie eine voll funktionsfähige Lösung erhalten.

- Abschnitt 6.4.1, „Datensynchronisierung“, auf Seite 48
- Abschnitt 6.4.2, „Zuordnen von Rollen“, auf Seite 48
- Abschnitt 6.4.3, „Konfiguration der Benutzeranwendung“, auf Seite 49
- Abschnitt 6.4.4, „Konfigurieren von Revision, Berichterstellung und Konformität“, auf Seite 49

6.4.1 Datensynchronisierung

Identity Manager verwendet Treiber zum Synchronisieren von Daten zwischen verschiedenen Anwendungen, Datenbanken, Betriebssystemen und Verzeichnissen. Nach der Installation von Identity Manager müssen Sie einen oder mehrere Treiber für jedes System konfigurieren, mit dem Sie Daten synchronisieren möchten.

Zu jedem Treiber gibt es ein Handbuch, in dem die Anforderungen und Konfigurationsschritte erläutert werden, die zum Synchronisieren der Daten erforderlich sind. Die Treiberhandbücher befinden sich auf der Dokumentations-Website für Identity Manager 4.0.1 Treiber (http://www.novell.com/documentation/idm401drivers/index.html).

Verwenden Sie das entsprechende Treiberhandbuch für jedes verwaltete System, um den Treiber zum Synchronisieren der Identitätsdaten zu erstellen.

6.4.2 Zuordnen von Rollen

Wenn Sie Informationen haben, die zwischen den verschiedenen Systemen synchronisiert werden müssen, verwenden Sie den Rollenzuordnungsadministrator zum Verwalten der Rollen in den verschiedenen Systemen. Weitere Informationen finden Sie im *Benutzerhandbuch zum Novell Identity Manager-Rollenzuordnungsadministrator 4.0.1*.

6.4.3 Konfiguration der Benutzeranwendung

Im nächsten Schritt fügen Sie mit der Benutzeranwendung eine Geschäftsperspektive zur Identity Manager-Lösung hinzu. Mit der Benutzeranwendung können Sie folgende Geschäftsanforderungen erfüllen:

- Anbieten einer praktischen Möglichkeit, rollenbasierte Bereitstellungsaktionen durchzuführen.
- Sicherstellen, dass Ihr Unternehmen über eine Methode verfügt, mit der es verifizieren kann, dass die Mitarbeiter die Unternehmensrichtlinien kennen und die erforderlichen Schritte unternehmen, um diese Richtlinien einzuhalten.
- Bereitstellen von Selbstbedienungsfunktionen, mit denen ein neuer Benutzer sich selbst registrieren kann, und Gewähren von Zugriff für anonyme oder Gastbenutzer.
- Sicherstellen, dass der Zugriff auf Unternehmensressourcen die organisatorischen Richtlinien erfüllt und dass die Bereitstellung im Kontext der Sicherheitsrichtlinie des Unternehmens erfolgt.
- Reduzierung des Verwaltungsaufwands für das Eingeben, Aktualisieren und Löschen von Benutzerinformationen über alle Systeme des Unternehmens hinweg.
- Verwalten der manuellen und automatisierten Bereitstellung von Identitäten, Diensten, Ressourcen und Assets.
- Unterstützung komplexer Workflows.

Das *Rollenbasiertes Bereitstellungsmodul für Identity Manager 4.0 Benutzeranwendung: Administrationshandbuch* enthält Informationen zur Konfiguration dieser Funktionen der Benutzeranwendung.

6.4.4 Konfigurieren von Revision, Berichterstellung und Konformität

Der letzte und wichtigste Schritt beim Erstellen einer Identity Manager-Lösung besteht in der Konfiguration der Revisions-, Berichterstellungs- und Konformitätsfunktionen, um sicherstellen zu können, dass die Lösung Ihre Unternehmensrichtlinien einhält. Ziehen Sie folgende Handbücher für die Einrichtung und Konfiguration dieser Funktionen zu Rate:

- **Revision:** *Identity Manager 4.0.1 Berichterstellungshandbuch für Novell Sentinel*.
- **Berichterstellung:** *Handbuch zum Identitätsberichterstellungsmodul* und *Verwenden von Identity Manager 4.0 Berichten*.
- **Konformität:** Siehe „Verwendung der Registerkarte „Konformität““ im Handbuch *Rollenbasiertes Bereitstellungsmodul für Identity Manager 4.0 Benutzeranwendung: Benutzerhandbuch*.

6.5 Identity Manager verwalten

Wenn Ihre Identity Manager-Lösung vollständig ist, stehen viele Handbücher zur Verfügung, die Ihnen bei der Verwaltung, Pflege und Änderung Ihrer Identity Manager-Lösung entsprechend den sich ändernden und wachsenden Geschäftsanforderungen helfen. Die verschiedenen Administrationshandbücher sind auf der Identity Manager 4.0.1 Dokumentations-Website (http://www.novell.com/documentation/idm401/index.html) im Bereich „Administration“ zu finden.