



Novell Identity Manager 3 als Directory- basierte Lösung bei Aegis Media

Nutzen und Notwendigkeit des Identitätsmanagement (Identity Management) sind unbestritten: Zum einen spart es Zeit und Kosten, personenbezogene Daten konsistent, ständig verfügbar und verlässlich bereitzuhalten. Zum anderen zwingen länderspezifische Vorgaben und Gesetze dazu, digitale Identitäten in entsprechender Weise zu behandeln.

Aegis Media, ein Unternehmen mit 400 Firmen in 70 Ländern, hat sich dieses Themas nicht nur von der technischen, sondern insbesondere von der inhaltlichen Seite genähert. Da die einzelnen Niederlassungen zum Teil mit elektronischem Personalsystem, zum Teil nur mit Excel-Sheets arbeiteten, galt es, die optimale Lösung sowohl für die größeren, als auch die ganz kleinen unter den Unternehmensstandorten zu finden.

Jedes stark wachsende, multinationale Unternehmen muss sich ähnlichen Herausforderungen stellen: Gesteigerte Anforderungen an Prozesse und die gesicherte Verfügbarkeit von Informationen für Mitarbeiter erfordern Systeme, die zuverlässige und gut strukturiert verteilte Informationsflüsse liefern. Die Fähigkeit, die richtigen Informationen den richtigen Personen zum richtigen Zeitpunkt zur Verfügung zu stellen, ist ein Schlüssel zum Erfolg.

Das Thema Identity Management wurde durch das „Aegis Infrastructure Team“ (AIT) bereits in 2001 aufgegriffen. Dieses Team, bestehend aus den IT-Verantwortlichen der einzelnen Regionen, fokussierte sich am Anfang auf das User Account Management (UAM). Einige IT-Manager hatten sich bereits mit den möglichen Lösungen, auch für den Bereich Identity Management, vertraut gemacht - dies jedoch mit „Technik-Brille“. Der Leiter des Teams trug diese Thematik ins Unternehmensmanagement und konnte die Entscheider davon überzeugen, einen übergeordneten Ansatz zu wählen und ein Konzept für ein umfangreiches Identity Management für den gesamten Konzern zu genehmigen. Die Vorteile lagen eindeutig auf der Business-Seite, nicht nur, was Zeit- und Kostenersparnis anbelangte. Ein weiterer wichtiger Aspekt war das Thema „Compliance“ mit den entsprechenden Kontroll- und Dokumentationsanforderungen. Gesetzliche Auflagen wie die EU-Richtlinie zum Datenschutz oder auch der Sarbanes-Oxley Act (SOX), der im Juli

2002 vom amerikanischen Kongress verabschiedet wurde, erfordern es, Compliance-Auflagen nicht nur regional anzugehen, sondern einen globalen und zukunftsorientierten Ansatz zu verfolgen.

Michael Ruppert, Director IT Operations Central Europe & Africa bei Aegis Media in Wiesbaden kontaktierte den langjährigen IT-Dienstleister des Unternehmens, Carpe diem aus Wiesbaden. Er ist unter anderem auf die Implementation von Directory-Services spezialisiert und konnte schnell aufzeigen, welche Vorteile von Identitätsmanagement sich für Aegis Media bieten. Zudem hatte Carpe diem bereits bei einem anderen großen multinationalen Unternehmen eine ähnliche Lösung implementiert und konnte entsprechende Expertise vorweisen.

Nach Evaluierung etlicher Lösungen entschieden sich die Verantwortlichen bei Aegis Media für den Novell Identity Manager, eine Lösung für plattformübergreifendes Identity Management und Provisioning. Dies

entsprach auch den Empfehlungen der Berater von Carpe diem, denn für ein Unternehmen, das sich durch Zukäufe und organisches Wachstum kontinuierlich verändert und vergrößert, bedarf es einer Lösung mit höchstmöglicher Flexibilität

Ein direkter Kontakt zu Novell Consulting USA untermauerte diese Entscheidung, so dass die Verantwortlichen im europäischen Headquarter in London Ende 2003 den Auftrag erteilten, als erste Phase des Projektes einen Prototypen zu entwickeln, der zu einer neuen und weltweit einsetzbaren Lösung für das Unternehmen führen sollte.

Die technische Seite

Anwenderkonten von Hand einzurichten kostet Zeit und Geld. Aber das ist nicht das einzige Problem: Ohne Automation entstehen Inkonsistenzen in der Handhabung von Regeln. Ein Provisioning-System führt zu besserer Prüffähigkeit und reduziert dadurch Risiken bei der Si-

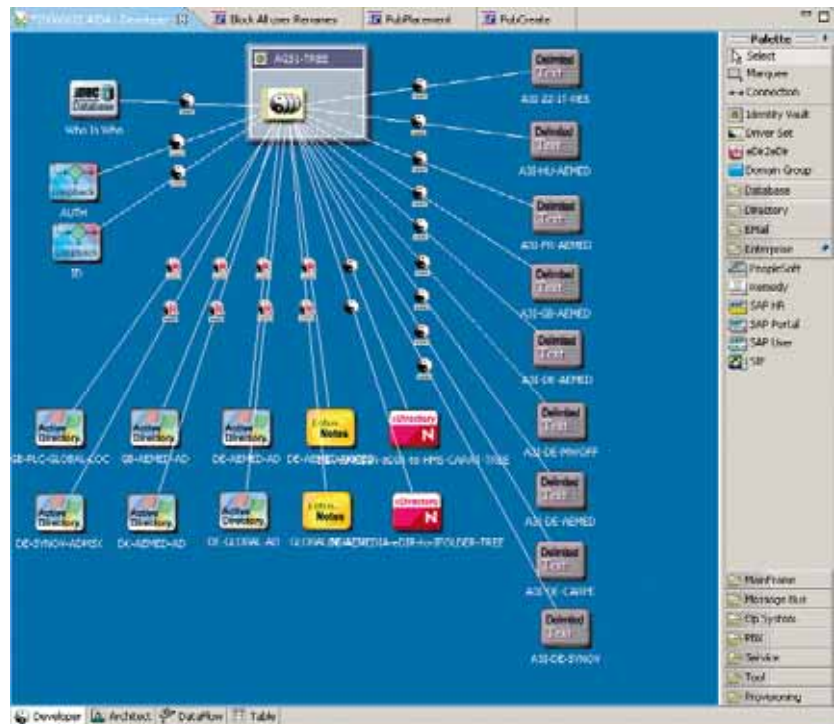


Bild 1: Der Identity Manager enthält ein flexibles, leistungsfähiges Modellierungswerkzeug, den Designer.

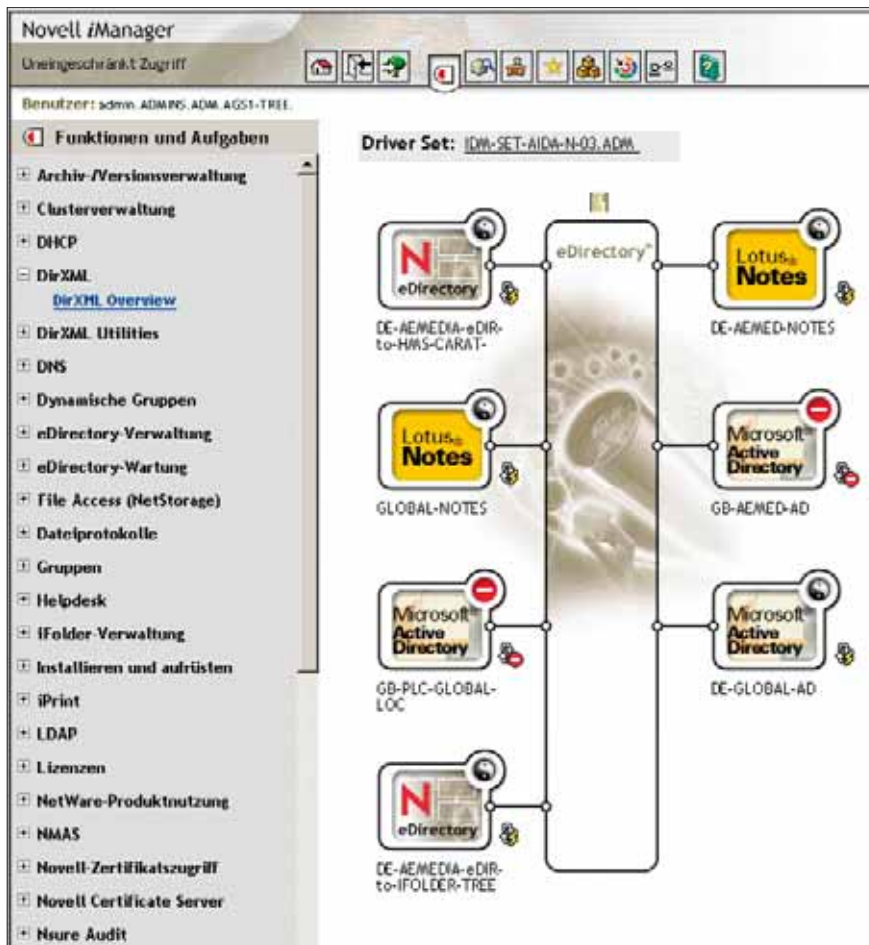


Bild 2: Ziele und Quellen als Überblick im Identity Manager Web basierenden Verwaltungstool.

cherheit und der Einhaltung von Richtlinien. Mit der Directory-basierten Lösung von Novell lässt sich eine IT-Infrastruktur aufbauen, der Rollen und Regeln für Anwender und Netzwerk-Ressourcen zugrunde liegen. Damit bekommen Anwender anhand von User-Informationen, verwendeten Geräten (etwa PDA oder Notebook) und Standort (im Firmenetz hinter der Firewall, per VPN von außen angemeldet, ungesicherter Dial-in, etc.) eine digitale Identität mit bestimmten Rechten ausge-

stellt. Anhand dieser Identität wird der Zugriff auf bestimmte Dienste gewährt, oder eben nicht. Das Entscheidende ist nicht das Identity Management an sich, sondern das so genannte „Identity Driven Environment“, in dem Dienste aller Art die digitale Identität der Nutzer auswerten. Damit wird die Sicherheit und Effizienz von Unternehmensnetzwerken erhöht und deren Administration wesentlich vereinfacht.

„Die technische Seite ist nicht unbedingt das Problem, denn die ge-

wählte Lösung ist lediglich der Enabler“, erläutert Ruppert. „Identitätsmanagement ist eher im Bereich Human Resources (HR) angesiedelt und weitaus komplexer, als man zunächst annehmen mag.“ Es galt also, die Personalabteilungen der einzelnen Niederlassungen für die Idee zu gewinnen und die Prozesse insgesamt zu harmonisieren.

Die Ausgangslage: Inkonsistente Datenpools aus 70 Ländern

Die Mitarbeiterdaten beim weit verzweigten Unternehmen Aegis Media wurden auf unterschiedliche Art gehalten und gepflegt: Deutsche Niederlassungen nutzten beispielsweise das SAP HR-Modul, Frankreich agierte mit einer selbst programmierten Access-Anwendung, Dänemark und Großbritannien hingegen arbeiteten mit Excel-Sheets, um nur einige europäische Länder zu nennen. Viele unterschiedliche User-Namen, unzählige Passwörter und falsch erfasste Daten verschärften das Problem. Genau genommen gab es im gesamten Konzern keine einzige übergeordnete Stelle, die über alle beschäftigten Mitarbeiter, deren Status und die Zugriffsberechtigungen exakte Informationen besaß. Ein aktuelles und detailliertes globales Reporting war so sehr schwierig und extrem aufwändig.

Die Idee: Citrix-basierte Lösung mit neuem Eingabe-Interface

Die neue Lösung musste die Ausgangslage in allen, unterschiedlich großen Firmen der Aegis Media Hol-



„Identitätsmanagement ist eher im Bereich Human Resources angesiedelt und weitaus komplexer als man zunächst annehmen mag.“

Michael Ruppert, Director IT Operations Central Europe & Africa bei Aegis Media

Info

Prozessgruppen des Identity Management

Identity Administration

Verwalten von digitalen Personenidentitäten, ihren Beziehungen zur Organisationseinheit und die Zuweisung von Ressourcen.

- **Existence** – Erzeugen, Verwalten, Synchronisieren von digitalen Personen-Identitäten.
- **Context** – Verwalten der Beziehungen von Personen zur Organisation (Rollen) und ihren Ressourcen (Rechte).
- **Provisioning** – Versorgen von Personen mit den ihrer Rolle entsprechenden Ressourcen und einbringen der Zugriffsrechte in die Zielsysteme, die die Ressourcenzugriffe steuern.

Community Management

Authentisierung, Bereitstellen / Publizieren und Autorisierung von Personen gemäß ihren digitalen Personenidentitäten.

- **Authentication** – Authentisierung, ist der Prozess der Verifikation der Identität anhand von Zertifikaten im allgemeinen Sinne.
- **Rendezvous** – Die unter Rendezvous zusammengefasste Prozessgruppe, umfasst das Zusammenstellen und Publizieren von Adressbüchern, Verzeichnissen, Kalenderfunktionen für Terminvereinbarungen, Online-Meetings und gemeinsamer Ressourcennutzung.

- **Authorization** – Autorisierung ist der Prozess, Personen gemäß ihrer digitalen Personenidentität (Existence) und der über ihre Rolle im Unternehmen definierten Zugriffsrechte (Context) den Zugriff auf Ressourcen zu gestatten oder zu verweigern.

Identity Integration

Mechanismen für die Aktualisierung und Synchronisation von digitalen Personenidentitäten, die verteilt und teilweise redundant gehalten werden.

- **Connection** – Mechanismen, die Eigenschaften von Verteilung und Heterogenität überwinden helfen. Technisch sind das Konnektoren zum Zugriff auf Standard Verzeichnisse (z.B. LDAP, DAP, ANS-SQL) oder Nicht-Standard-Verzeichnisse.
- **Brokerage** – Mechanismen, die es gestatten Attribute unterschiedlicher Informationsobjekte aufeinander abzubilden. Technisch realisiert über eine Regelmaschine, die auf einem Satz definierter Abbildungsregeln operiert.
- **Ownership** – Mechanismen, die bei redundant gespeicherten Informationsobjekten festlegen (und überwachen), in welcher (autoritativen) Quelle bestimmte Attribute führen geändert werden dürfen.

Prozesse des Identity Management

Anwender (Existence)

- Hinzufügen eines Anwenders
- Entfernen eines Anwenders
- Ändern eines Anwenders (Name, Abteilung, Vertragsende)

Rolle (Context)

- Hinzufügen einer Rolle (und Zuweisen der damit verbundenen Rechte, auch über „Klonen“ oder über Vorlagen/Templates)
- Entfernen einer Rolle (auf die keine Referenz mehr existiert)
- Ändern einer Rolle.
- Prüfen auf Konfliktfreiheit

Konto (Context)

- Vergeben individueller Rechte,
- Entziehen individueller Rechte,
- Zuordnen zu einer Rolle
- Lösen von einer Rolle
- Konten unwirksam werden lassen (Ausscheidatum erreicht)
- Wiederinkraftsetzen abgelaufener Konten (Ausscheidatum erreicht) Passwort setzen (Initial-Passwort und Neuvergabe)

Regel (Context)

- Hinzufügen einer Regel
- Entfernen einer Regel
- Ändern einer Regel
- Genehmigungsstellen (Provisioning)
- Hinzufügen einer Freigabeautorität (mit Vertretungsregelung),
- Entfernen einer Freigabeautorität,
- Ändern einer Freigabeautorität,

Information (Provisioning)

- Information des Anwenders über eigene Zugriffsberechtigungen
- Information des Verantwortlichen über die Zugriffsberechtigungen Dritter (nach Systemen, Organisationseinheiten),
- Information des Anwenders über den Status eines Antrages auf Rechtevergabe,

Abgleich (Provisioning)

Feststellen von Abweichungen der Berechtigungen in den Zielsystemen vom Sollzustand (Hacker, Prozessmängel, Managementfehler, ...)

ding berücksichtigen. „Es bot sich an, eine Citrix-basierte Lösung zu nutzen“, erklärt Harald Gemmer, Geschäftsführer von Carpe diem. „Anwendungen und Informationen liegen auf einem zentralen Server und lassen sich mit Citrix nach Bedarf, also „on demand“, bereitstellen. Es ist nicht mehr notwendig, die einzelnen Applikationen auf den Endgeräten zu installieren. Mit einer eigens entwickelten Applikation und benutzerfreundlichem Eingabe-Interface, AIDA Local, lassen sich die Mitarbeiterdaten direkt in AIDA (Aegis Identity Directory Architecture) einspeisen und werden per Mausklick aktuell und zentral bereitgestellt.“

Mit AIDA zum Erfolg

Da der durch Carpe diem entwickelte Prototyp von AIDA alle Beteiligten überzeugte, wurde im Mai 2004 die Phase 2, ein umfangreiches Pilotprojekt, zügig in Angriff genommen. Zunächst wurden diejenigen Länder identifiziert, die den Proof-of-Concept durchführen sollten. Die Wahl fiel auf einen Länder-Mix mit den unterschiedlichen vorhandenen Ausgangsvoraussetzungen, insgesamt 5 Länder mit 70 Niederlassungen. Sollte das Pilotprojekt bis Juni 2005 die gewünschten Ergebnisse bringen, war in Phase 3 und 4 der Rollout über alle 70 Länder mit den einzelnen Unternehmensstandorten ge-

Info

Carpe diem GmbH

Kreative Lösungen + einfache Wege!

Carpe diem ist Dienstleister für die Planung und die Realisierung von technischen und organisatorischen IT-Anforderungen. Partnerschaften sind unter anderem: Citrix Gold, Novell Platinum und Microsoft Certified Partner. Ein Themenschwerpunkt ist die Projekt Entwicklung und Implementation von Identity Management Systemen.

The Only Constant Is Change.
www.carpediem.de

plant. Auch ein Finetuning über alle Phasen hinweg war mit im Plan. Parallel dazu mussten erweiterte Namenskonventionen entwickelt werden, um den Gegebenheiten in allen Ländern Rechnung zu tragen. Benutzer heißen nämlich oftmals anders, als sie in den IT-Systemen auftreten. Dies erwies sich als echte Sisyphus-Arbeit.

Der Teufel steckt im Detail

In einem multinationalen Unternehmen mit asiatischen Niederlassungen können ganz spezielle Probleme auftreten, beispielsweise mit japanischen Mitarbeitern: Die meisten japanischen Vornamen werden mit sogenannten Kanji-Schriftzeichen geschrieben, die ursprünglich aus China stammen und von denen jedes Zeichen für sich bereits ein gan-

zes Wort bedeutet. Die meisten Namen werden mit zwei Kanji geschrieben, manche mit drei, einige aber auch nur mit einem. Diese Vornamen haben ganz spezielle Bedeutungen und können meist gar nicht in westliche Namen „übersetzt“ werden. Japanische Familiennamen stehen traditionell vor dem persönlichen Namen. Wird der Name in Kanji geschrieben, steht er daher immer in dieser Reihenfolge. In westlicher Schrift wird er hingegen in der Regel mit Vorname und Nachname geschrieben und muss „lokalisiert“ werden, also in ein „Pseudonym“ verwandelt. Im Pass, in der Personalakte oder in der Email-Adresse finden sich dann völlig unterschiedliche Namen wieder.

Aber auch Europa kann mit Namensproblemen aufwarten: Wie werden Adelstitel behandelt? Wie wird das häufig auftretende „van“ in niederländischen Nachnamen berücksichtigt? Wie geht man mit Doppelnamen um, die in den einen Systemen geführt werden, in den anderen hingegen nicht? Der Dokortitel ist Bestandteil des Namens, wie wird dies gehandhabt?

Man einigte sich in Absprache mit den Human Resources-Abteilungen, einen pragmatischen Ansatz zu verwenden: Standardisierung soweit möglich – individuelle Lösungen in Absprache mit den jeweiligen Personalabteilungen. In der Phase 3 des Projektes wird nun das Thema „extended international and translated naming“ detaillierter behandelt. „Ex-

Info

Identity Management und Provisioning mit Identity Manager von Novell

Novell ist ein führender Anbieter im Markt für Identity Management-Lösungen und hat mit Novell Identity Manager eine Lösung für plattformübergreifendes Identity Management und Provisioning im Portfolio. Unternehmen erhalten damit vereinfachte Kontrolle über den Zugriff durch die Anwender, erhöhen den Schutz sensibler Daten, senken administrative Kosten und halten gesetzliche und unternehmensweite Richtlinien ein. Novell Identity Manager bietet eine verbesserte Visualisierung und zusätzliche Funktionen, um Workflows zu bearbeiten, Freigabeprozesse zu automatisieren und als Endanwender selbst Ressourcen zu beschaffen und Berechtigungen anzufragen.

Mehr Informationen unter:
<http://www.novell.com/de-de/solutions/securityandidentity>

tended“ geht davon aus, dass der reale Name, der im Ausweis steht, genutzt wird – selbst wenn es Kanji-Code ist. Dann kann der Mitarbeiter mit HR verhandeln, ob und wenn ja, welchen Alias-Namen er annehmen möchte.

Da auch das Thema Datenschutz in den einzelnen Ländern unterschiedlich gehandhabt wird, ist das neue System flexibel genug angelegt, um sich mit den jeweiligen Gesetzen arrangieren zu können.

Ein Mausklick entscheidet über den Zugriff

Das Projekt „Identity Management“ ist nun so weit fortgeschritten, dass deutliche Ergebnisse sichtbar sind: Das Pilotprojekt erweist sich als voller Erfolg. Viele Abläufe konnten

auch zusätzliche Attribute (beispielsweise Email-Adressen) beinhalten. „Die Möglichkeit, aus verschiedenen Quellen Informationen in das Metadirectory einzuspeisen und HR ein entsprechend umfangreiches Reporting anbieten zu können, war im Übrigen den Personalabteilungen gegenüber ein „Hauptverkaufspunkt“ für unsere neue Lösung.“, berichtet Ruppert.

Nutzen bereits sichtbar

Die Ergebnisse des Projektes sind sehr ermutigend und der Nutzen bereits sichtbar, denn aus den einzelnen HR-Abteilungen kommen nun valide und sichere Daten, die zentral zur Verfügung gestellt werden können. Auch die Zeit- und Kostenersparnis sind spürbar. Viele

das Projekt, so Ruppert, bleibt ein lebender und sich ständig weiterentwickelnder „Organismus“. „Die nächsten Schritte werden wir selbstverständlich weiterhin mit Carpe diem gehen, denn hier haben wir bereits seit vielen Jahren einen verlässlichen Partner gefunden, sowohl für Infrastrukturthemen als auch in der Beratungsleistung. Gerade in diesem Projekt haben die Mitarbeiter von Carpe diem bewiesen, dass sie nicht nur die Technik-Seite, sondern in besonderem Maße auch die Business-Seite verstehen und so gemeinsam mit uns zu optimalen Lösungen gekommen sind“, resümiert Ruppert.

Ulrike Meinhardt



„Der IT-Dienstleister muss ein IdM-Projekt von der Technik- und der Business-Seite her verstehen und angehen.“

bereits teil-automatisiert werden und laufen daher spürbar reibungsloser ab. Neue Mitarbeiter sind schneller produktiv, da die benötigten Ressourcen auf Mausklick aktiviert und bereitgestellt werden können. Was jedoch genauso wichtig ist: Scheidet ein Mitarbeiter aus, kann sein Zugriff ebenfalls auf Knopfdruck gelöscht, beziehungsweise deaktiviert werden: Das Einloggen im Netzwerk ist nicht mehr möglich, die Stechkarte funktioniert nicht mehr, der Zugriff auf unternehmenskritische Daten ist komplett unterbunden.

Das Reporting ist nun ebenfalls automatisiert. Durch die Kopplung der Daten aus HR und den angeschlossenen Systemen lassen sich nun Listen generieren, die sowohl die Mitarbeiterinformationen als

Einzelaspekte werden jedoch in den kommenden Monaten, parallel zum Rollout über das gesamte Unternehmen, hinzukommen. So möchte Michael Ruppert, Leiter IT Operations bei Aegis Media, noch zusätzliche Informationen in das System mit einbinden, zum Beispiel die Zuordnung zu einzelnen Kunden. Da derzeit noch kein Single-Sign-on möglich ist, wird auch dieser Punkt in den nächsten Schritten mit berücksichtigt. Auch im Bereich der Passwort-Vergabe soll eine Änderung stattfinden. Wo jetzt das Passwort top-down für alle Anwendungen von AIDA kommt, soll es in Zukunft auch möglich werden, Passwörter direkt an AIDA zurückzuspielen, wenn ein Benutzer dies in einem System ändert.

Es bleibt also noch viel zu tun und

**Sie sind
umgezogen?**

Dann senden Sie uns bitte ein
Fax an 08104 6494-22 oder eine
eMail an neff@it-verlag.de