Meta Directory – integrierendes Element in einer verteilten, heterogenen IT/TK-Landschaft

Jörg Deutschmann

Technische Universität Ilmenau
Universitätsrechenzentrum
Joerg.Deutschmann@RZ.TU-Ilmenau.DE

Kurzfassung. Meta Directory, das neue Paradigma im Bereic h der Verzeich - nisdienste, verspricht ein hohes Integrationspotential. Im Netzwerklabor der Technischen Universität Ilmenau konnten erste Erfahrungen beim Einsatz eines integrierenden Verzeichnisdienstes gesammelt werden. Der in diesem Beitrag vorgestellte Prototyp für ein Corporate Directory an der Technischen Univer - sität Ilmenau verdeutlicht die Vorgehensweise bei der Einführung eines Meta Directory und zeigt die Probleme sowie erste Ansätze zu deren Lösung auf.

1 Motivation

Die gestiegene Komplexität von IT - und TK -Systemen führt dazu, dass kaum ein Administrator mehr in der Lage ist, diese zu beherrschen. In ihrer Gesamtheit betrachtet, gehören hierzu die Rechner - und Telefonnetze von der Verkabelung über das aktive Equipment bis hin zu den Anwendunge n und ihren Benutzern. In der Praxis erfolgt eine Aufteilung der Verantwortlichkeiten in Abhängigkeit von der Kompetenz der beteiligten Mitarbeiter. Dabei besteht die Gefahr, dass die Administration der entstandenen Teilbereiche zu stark auseinander läuft. Zusammenhänge gehen verloren, wenn in den einzelnen Bereichen für sich mächtige aber nach außen abgeschlossene Werkzeuge zum Einsatz kommen.
Um ein gravierendes Beispiel handelt es sich bei der Verwaltung von Benutzern in einer heterogenen Rechnerumgebun g. Im schlimmsten Fall müssen die Änderungen jeglicher Benutzerdaten in allen beteiligten Systemen von Hand nachgeführt werden. Auch im Zusammenhang mit der Verwaltung von Netzwerk - und Telekommunika - tionsressourcen ist eine mangelnde Integration bei den f ür die Administrations - prozesse verantwortlichen Komponenten, den Datenbanken und Applikationen, zu verzeichnen [4].
Die isolierte und dezentrale Verwaltung von systemübergreifenden Informationen beschwört Redundanzen, Inkonsistenzen und Sicherheitslücken herauf. Zur Erhöhung der Benutzerfreundlichkeit und zur Erleichterung der Administration in einer zunehmend zusammenwachsenden IT - und TK -Welt ist eine integrierende Ressourcenverwaltung notwendig, in der alle systemübergreifenden Informationen zur Verfügu ng stehen. Das damit verbundene Integrationspotential kann nur durch einen offenen und anerkannten Standard sichergestellt werden. Aufgrund eines stabilen Standardisierungsprozesses sowie einer breiten Unterstützung durch die

Hersteller rücken Verzeichnisd ienste immer mehr in den Mittelpunkt der Ressourcenverwaltung für verteilte, heterogene Umgebungen.

2 Directories und ihr Integrationspotential

Verzeichnisse besitzen aufgrund ihrer Eigenschaften und diverser Erweiterungen ein hohes Integrationspotential . Um dieses Potential ausschöpfen zu können, ist jedoch ein nicht zu unterschätzender Entwicklungsaufwand bei der Integration notwendig.

2.1 Allgemeine Eigenschaften von Directories

Verzeichnisse sind optimiert für das Nachschlagen von Informationen. Als Rechneranwendung handelt es sich um einen Dienst, der die Suche von und in hierarchisch strukturierten Daten erlaubt [1]. Die Objekte der realen Welt werden in einem Verzeichnis, also relativ unabhängig voneinander, innerhalb einer Hierarchie abgebildet. Der Aufbau der Hierarchie bzw. des Verzeichnisbaumes definiert die grundlegenden Beziehungen zwischen den Objekten [2]. Die Attribute der Objekte besitzen definierte oder sogar standardisierte Namen.
Der Zugriff auf Verzeichnisse erfolgt heute über das *Lightweight Directory Access Protocol* (LDAP). LDAP ist zunächst ein offen standardisiertes Zugriffsprotokoll für Verzeichnisse. Außerdem entwickelt sich im Rahmen von LDAP ein für verschiedene Anwendungsfälle geeignetes Kernschema. Auch die Entwicklungen im B ereich Directory-enabled Network lassen die Bedeutung von Verzeichnisdiensten und LDAP weiter wachsen [3].
Verzeichnisdienste eignen sich für einen offenen Zugriff, einen verteilten Ansatz sowie für Anwendungen mit häufigen Lese - und Suchoperationen. Aufgr und der Komplexität jeder einzelnen Anwendung ist die Einführung einer integrierenden Benutzer- und Ressourcenverwaltung immer mit einem nicht zu unterschätzenden Aufwand an Eigenentwicklung verbunden. Gesucht wird deshalb ein Rahmenwerk, dass die Integrat ion unterschiedlicher Verzeichnisse und anderer Informations - ressourcen innerhalb einer Universität, einer Organisation oder eines Unternehmens zu einem einzelnen globalen Verzeichnis gestattet und unterstützt. Für dieses globale Verzeichnis prägten Marktf orschungsinstitute vor etwa drei Jahren den Begriff Meta Directory bzw. Full-Service Directory [4].

2.2 Meta Directory und Konnektoren

Der Begriff Meta Directory steht für ein neues Paradigma in der Welt der Verzeichnisdienste. Der integrierende Ansatz e ines Meta Directory verleiht dem verteilten System, bestehend aus unterschiedlichen Verzeichnissen und anderen Informationsressourcen, einen zentralisierten Charakter [6]. Den Übergang zu jeglichen Informationsressourcen stellen sogenannte Konnektoren sich er. Die Konnektoren eines Meta Directory enthalten die Übergangslogik für die Integration unterschiedlicher Informationsressourcen. Konnektoren bestehen ganz grob aus einer

LDAP-Komponente zur Kommunikation mit Verzeichnissen, aus einem API zur Programmierung notwendiger Erweiterungen sowie aus einem programmierbaren Regelwerk zur flexiblen Spezifikation von Übergangslogik und notwendigen Konvertierungen. Neben der standardkonformen Umsetzung für LDAP, der Universalität der verwendeten Skriptsprache, der Mächtigkeit der Synchronisierungs-, Partitionierungs- und Replikationsmechanismen sind die verfügbaren Konnektoren für die Auswahl eines geeigneten Meta Directory von entscheidender Bedeutung. Durch die Integration unterschiedlichster Anwendungen mit Hilfe der Konnektoren geht die Einführung eines Meta Directory immer mit einer gründlichen Analyse der Geschäftsprozesse einher, was die Vorgehensweise hierbei maßgeblich beeinflusst.

2.3 Vorgehensweise beim Einsatz von Meta Directories

Die Vorgehensweise für die Einführung eines Meta Directory geht nach [5] von einer gründlichen Analyse der Informationsquellen und der darauf aufsetzenden Anwendungen aus. Im Ergebnis der Analysephase sollten nicht nur konkrete Anforderungen definiert sondern vor allem auch Priorisierungen für die Integration der einzelnen Informationsressourcen vorgenommen werden. Dies geschieht im Einklang mit der Bedeutung und den Abhängigkeiten der Ressourcen.
Der Entwurfsprozess für ein Meta Directory ist durch zwei wichtige Schritte gekennzeichnet – der Entwurf des Verzeichnisbaumes und die Spezifikation für die Konnektoren. Der Entwurf des Verzeichnisbaumes (*Directory Information Tree*) umfasst Festlegungen zur Struktur in Abhängigkeit von Partitionierung, Replikation und Administration, Festlegungen zur eindeutigen Identifikation von Objekten innerhalb des Verzeichnisses (*Distinguished Names*), Namenskonventionen sowie die Entscheidung für zu verwendende Objektklassen und ihre Attribute. Die Spezifikation der Konnektoren legt das Regelwerk für den Übergang in die Zielsysteme fest und definiert die erforderlichen Import-, Export- und Synchronisationsfunktionen.
Zum Teil parallel können die Auswahl des passenden Meta Directory sowie erste Testinstallation und das Prototyping erfolgen, um dann die Umsetzung des Entwurfs nach produktspezifischen Gegebenheiten und die schrittweise Integration der Zielsysteme vornehmen zu können.

3 Corporate Directory der Technischen Universität Ilmenau

Die Entwicklung eines Corporate Directory an der Technischen Universität Ilmenau basiert auf dem Paradigma des Meta Directory und orientiert sich an der oben beschriebenen Vorgehensweise.

3.1 Zielsetzungen

Mit der Einführung eines integrierenden Verzeichnisses zur Verwaltung von Benutzern und anderer Ressourcen an der TU Ilmenau werden vor allem drei Hauptziele verfolgt. Die Arbeit der Administratoren soll sich durch eine zentralisierte

Sicht auf den Datenbestand, was auch als *Single Point of Administration* bezeichnet wird, und die Einführung entsprechender Werkzeuge erleichtern. Ein zweiter Punkt befasst sich mit dem Datenschutz und der Datensicherheit. Hierfür sind Richtlinien und Prozeduren zur sicheren Benutzung und Administration der Datenbasis aufzustellen, wie zum Beispiel die Vergabe von Berechtigungen und die Festlegungen für Replikationsfunktionen. An dritter Stelle steht die einheitliche Identifikation der Benutzer im Sinne von *Single Sign On* und damit die Verbesserung der Benutzer-freundlichkeit bei der Arbeit an unterschiedlichen Systemen. Der Weg zur Erreichung dieser Ziele ist Gegenstand einer umfangreichen Analysephase.

3.2 Analyse

Eine erste Analyse der bestehenden Informationsressourcen an der TU Ilmenau, insbesondere im Universitätsrechenzentrum, hat ergeben, dass die in Abbildung 1 dargestellten Anwendungen als Zielsysteme für eine Integration in Frage kommen.

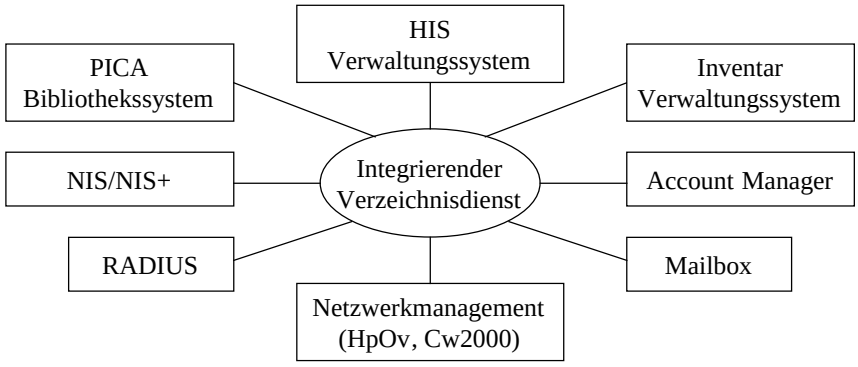


Abb. 1. Zielsysteme für eine Integration.

Die zentrale Verwaltung und die Prüfungsämter der TU Ilmenau verwalten die aktuellen Daten der Studenten im HochschulInformationsSystem (HIS) der HIS GmbH. Hieraus lassen sich die Informationen über Immatrikulationen und Exmatrikulationen entnehmen, um den Datenbestand der studentischen Benutzer aktuell zu halten. Die Benutzerdaten müssen dann mit weiteren Systemen abgeglichen werden. Im *Network Information System* (NIS/NIS+) sind die Unix-Benutzer des Rechenzentrums verzeichnet. Novells *Account Manager* stellt die Verwaltung der Anwender von Microsoft Windows sicher. Der *Remote Authentication Dial In User Service* (RADIUS) überwacht die Einwahl in das Netz der Universität per Modem oder ISDN. Jeder Benutzer kann und sollte auch über eine zentral vom Rechenzentrum verwaltete Mailbox verfügen, für die, neben einigen anderen Informationen, Benutzername und Passwort vorgehalten werden. Ebenfalls in die Rubrik Benutzerverwaltung fällt das Bibliothekssystem PICA. Die Mitarbeiter der Bibliothek verwalten hiermit die Bibliotheksbenutzer vollkommen abgekoppelt und redundant. Beim Netzwerkmanagement handelt es sich ebenfalls um ein weites Feld für die Einführung eines integrierenden Verzeichnisses. Router- und Switch-Konfigu-

rationen, Internetadressen und Domainnamen seien hier beispielsweise aufgezählt. Als Netzwerkmanagementsysteme befinden sich *HP Open View* (HpOv) und *Cisco Works 2000* (Cw2000) im Einsatz. Lösungsvorschläge in diesem Bereich kommen von der *Desktop Management Task Force* (DMTF) und von der Initiative *Directory Enabled Network* (DEN) [3]. Die Integration der Verwaltung des Inventars an der TU Ilmenau ist eine recht neue Anforderung für das Corporate Directory.
Die angesprochenen Systeme werden zur Zeit auf ihre Schnittstellen hin untersucht. Benutzerdaten und die Konfigurationsdaten des Netzwerks befinden sich in proprietären Datenbasen, aus denen über Perl-Scripts die entsprechenden Einträge für NIS/NIS+, den Account Mananger oder das Domain Name System (DNS) generiert werden. Der Prozess der Beantragung, beispielsweise für einen RADIUS-Account oder eine Internetadresse, ist zum Teil mit Medienbrüchen verbunden.

3.3 Verzeichnisbaum und Konnektoren

Der Entwurf des Verzeichnisbaumes und erste Festlegungen für die Konnektoren stellen wichtige Entwurfsschritte dar. Ein gut entworfener Verzeichnisbaum unterstützt eine einfache Datenpflege, eine flexible Definition von Zugriffsrechten und Verteilungsarchitekturen, eine Anbindung von Verzeichnisapplikationen sowie eine intuitive Navigation durch das Verzeichnis. Der Verzeichnisbaum muss den Anforderungen der TU Ilmenau entsprechen, also ihrer Organisationsstruktur. Er sollte es ermöglichen alle relevanten Informationen aufzunehmen, was sich auf die verwendeten Objektklassen, ihre Attribute und die Strukturregeln bezieht. Es ist davon auszugehen, dass ein Großteil der Benutzer- und Ressourcenverwaltung dem Universitätsrechenzentrum obliegt. Aber auch in den Fakultäten, zentralen Einrichtungen, Instituten und Fachgebieten verwalten Administratoren ihre Ressourcen. Im Sinne der Verteilungsstruktur sollte deshalb ein Kompromiss zwischen einem strukturorientierten und einem funktionell orientierten Ansatz gewählt werden. Die konkrete Ausprägung dieses Ansatzes befindet sich derzeit in der Diskussion. Für die Integration der Zielsysteme werden Konnektoren zum Zugriff auf SQL-fähige Datenbanken und auf strukturierte Dateien, die jedoch ohne Auszeichnungen (Tags) vorliegen, konfiguriert. Die Analyse der Zielsysteme ist an dieser Stelle noch nicht abgeschlossen.

4 Zusammenfassung und Ausblick

Im Netzwerklabor der TU Ilmenau existiert ein Prototyp für die verzeichnisbasierte Netzwerkadministration und Benutzerverwaltung. Bei seiner Realisierung konnten erste Erfahrungen gesammelt und zusammengefasst werden. Zum Entwurf des Verzeichnisbaumes sollte möglichst das Standardschema bzw. das mit dem Produkt gelieferte Kernschema zum Einsatz kommen, was vor allem zu einer guten Unterstützung im strukturellen Bereich führt. In diesem Zusammenhang sind weit verbreitete Verallgemeinerungen, wie zum Beispiel Common Name und Canonical Name, sehr hilfreich. In der Diskussion mit den verantwortlichen Administratoren zeigte sich, dass eine weitgehende Autonomie der angeschlossenen Teilsysteme

gewährleistet sein muss. Systemspezifisch sensible Daten sollten möglichst im Zielsystem verbleiben, systemübergreifende Informationen von allgemeinem Interesse gehören in das Meta Directory, um ein Optimum beim Aufwand für Partitionierung, Replikation und Synchronisation zu erreichen.
Das eingesetzte Produkt DirX Meta Directory von der Siemens AG [7] verfügt über einen X.500-konformen Verzeichnisdienst, läuft sehr stabil und kann unter Microsoft Windows und diversen Unix-Systemen zum Einsatz kommen. Partitionierung und Replikation sind mit X.500 standardisiert und bei DirX Meta Directory leistungsfähig umgesetzt, was bei reinen LDAP-Produkten zur Zeit noch proprietär ist. DirX Meta Directory verwendet die Tool Command Language (TCL) als Script-Sprache, die sich als sehr geeignet für den Prozess des Prototyping erwies. Außerdem bietet DirX Meta Directory ein leicht erweiterbares Rahmenwerk zur Entwicklung von Web-Benutzerschnittstellen. Das mit DirX Meta Directory gelieferte Kernschema lässt jedoch gerade im Bereich des Netzwerkmanagement zahlreiche Wünsche offen.
Für die Fortführung der Arbeiten wird ein umfangreiches Projekt mit nicht zu vernachlässigenden Investitionen erwartet. Der Entwurf der Ablaufstrukturen und die Spezifikation der Konnektoren geht mit einer gründlichen Analyse der Geschäftsprozesse einher. Deshalb nimmt eine universitätsinterne Arbeitsgruppe, bestehend aus Administratoren und anderen interessierten Mitarbeitern, die Analysearbeit auf. Weiterhin soll die universitätsübergreifende Zusammenarbeit, zum Beispiel mit der FH Schmalkalden, der Universität Erfurt und der Bauhaus-Universität Weimar weiter ausgebaut werden.
Im Rahmen des Corporate Directory der TU Ilmenau steht derzeit das Konfigurationsmanagement für das Netzwerk im Mittelpunkt der Betrachtungen. Weiterhin wird über eine Werkzeugunterstützung bei der Einrichtung der Konnektoren und eine möglichst automatische Auswertung von Schemainformationen aus dem Zielsystem mit nachfolgender dynamischer Schemaanpassung nachgedacht. Im Verlauf des Projekts sollte sich das Netzwerklabor der TU Ilmenau zu einem Kompetenzpunkt im Bereich Meta Directory entwickeln.

5 Literatur

[1] Timothy A. Howes; Mark C. Smith; Gordon S. Good. *Understanding and deploying LDAP directory services*. Macmillan Technical Pub, 1999

[2] Rob Weltman; Tony Dahbura. *LDAP programming with Java*. Addison-Wesley, 2000

[3] John Strassner. *Directory enabled networks*. Macmillan Technical Publ., 1999

[4] Jürgen Höfling. *Verzeichnisdienste (Teil 3) - Fehlanzeige bei Out-of-the-Box*. Information Week, Ausgabe 25, 26. Oktober 2000

[5] Hadi Stiel. *Meta Directories zur Integration von bestehenden Verzeichnissen - Planvolle Regie von oben*. NetworkWorld 21-00, 20.10.2000

[6] Martin Goldmann. *Meta-Directories - Datenquellen vereinigen*. PC Professionell, Ausgabe 10/2000

[7] Siemens AG; Information and Communications. *Dokumentation zu DirX Meta Directory*. http://www.siemens.com/directory/