Pläne zum Umstieg auf X.500 (93) mit Einbindung von Standalone LDAP Servern

Peter Gietz, Projekt DFN Directory Services,
Zentrum für Datenverarbeitung,
Universität Tübingen
email: peter.gietz@directory.dfn.de

PG 99-106v1
19. August 1999

Inhaltsverzeichnis

1 Status dieses Dokuments

Dieses Dokument ist als Diskussionsvorlage für das Betreibertreffen „Zukunft von Directories in Deutschland" gedacht, das am 1. und 2. September 1999 in Tübingen stattfinden wird. Eine endgültige Version dieses Textes wird nach diesem Treffen im WWW veröffentlicht. Kommentare sind willkommen.

2 Vorbedingungen

Die gegenwärtige internationale White Pages Directory Infrastrastruktur, wie sie im NameFLOW Pilot Projekt von DANTE[1] seit vielen Jahren betrieben wird, baut auf Directory System Agents der Quipu Software auf, eine proprietäre Implementierung des 88er X.500 Standards [1]. Gegenwärtig beteiligen sich 40 Länder an diesem Projekt. Daten von über 5.000 Organisationen sind im Directory eingetragen. Die Anzahl der Personeneinträge wird auf ca. 2 Millionen geschätzt.

Allerdings zeichnet sich, was die Beteiligung von Organisationen und die Datenmenge angeht, eine Stagnation ab. Außerdem ist die Qualität der Einträge sehr unterschiedlich. Viele Datenbestände sind einmal eingefahren worden und seit vielen Jahren nicht mehr gepflegt.

Ein weiteres Problem ist, daß die Quipu-Software nicht Jahr 2000 Kompatibel ist. Dies zwingt zu einer Erneuerung der Infrastruktur, wobei sich zwei Wege anbieten:

- Umstieg auf eine LDAP Infrastruktur
- Umstieg auf neuere X.500 Produkte, die dem 93er Standard folgen

3 LDAP Lösungen

LDAP hat sich von einem reinen Zugriffsprotokoll für X.500 zu einer eigenständigen Directory-Welt entwickelt. Die aktuelle Version (v3) [2, 3, 4] ermöglicht durch einen Referral-Mechanismus die Verweisung eines informationsuchenden Clients auf einen Server, der diese Information vorhalten könnte. Solche Referrals können in einem Server konfiguriert werden, um somit ähnlich der X.500 Welt einen Directory Information Tree nachzubauen. Referrals können aber auch automatisch erzeugt und in Indexsystemen Verwendung finden. Weitere Features, die von einem vollwertigen Directory-System erwartet werden, befinden sich gerade in der Entwicklung: Access Controll [5, 6], Authentifizierung [7] und Replikation [8, 9, 10].

Viele Länder nehmen diesen spürbaren Trend auf und bauen eine reine LDAP Lösung auf. So wurde in Schweden gerade im Rahmen des TISDAG Projektes ein Directory-Indizierungssystem aufgebaut, das LDAP und Whois++ Server miteinander verbindet[2] [11, 12, 13]. In Norwegen wird ein reines LDAP „Directory of Directories"

[1] siehe http://www.dante.net/np
[2] siehe http://tisdag.sunet.se/,

aufgebaut [14]. Auch Holland [3] und Griechenland[4] haben sich für reine LDAP-Lösungen entschieden.

Im Rahmen des EC-geförderten Projekts DESIRE II[5] wird ein Indexsystem auf Basis des Common Indexing Protocol (CIP) [15, 16, 17, 18] aufgebaut, das so skalierbar ist, daß es ein gesamteuropäischen Index aller LDAP-Server verwalten kann [19].

Auch in Deutschland gibt es viele Organisationen, die anstelle von X.500 zu LDAP-Lösungen greifen. Im Rahmen einer zwingend notwendig gewordenen Neustrukturierung der Directory-Infrastruktur, wird es unumgänglich sein, LDAP Server mit einzubeziehen.

4 X.500(93)

Frühere von DANTE durchgefürte Interoperabilitätstest [20, 21] verschiedener 93er X.500-Produkte haben etliche Schwierigkeiten aufgezeigt, insbesondere auf dem Gebiet der Replikation. Allerdings sind seit diesen Test mehrere neue Versionen der verschiedenen Implementationen erschienen und neue Tests, die eventuell bald im Rahmen der Open Group[6] durchgeführt werden, könnten aufzeigen, daß diese Interoperabilitätsprobleme der Vergangenheit angehören. Dennoch hat man sich international darauf geeinigt, ein Backbone von First-Level-DSAs nur eines Softwareherstellers aufzubauen, um solchen Problemen aus dem Weg zu gehen. Die Wahl ist hierbei auf den LDAP/X.500 Enterprise Directory Server der Firma Messaging Direct gefallen, der nunmehr in einer Version 5 vorliegt[7]. Ein Grund für diese Produkt war die zunehmende Integration von LDAP Funktionalität in den X.500 Server.

Ein Problem, daß sich bei einem Umstieg von dem 88er Standard auf den 93er Standard ergibt, ist der im Standard selbst nicht vorgesehene RootDSA oder Root Context. Dieser hat sich in der Quipu-Infrastruktur bewährt bei der Koordinierung der Replikation der verschiedenen First-Level-DSAs. Ein Versuch den Root-Context in die 93er rüberzuretten [22], muß als fehlgeschlagen angesehen werden, da er auf das Directory Operational Protocol (DOP) basiert, welches bisher wegen seiner Komplexität von keinem Softwarehersteller implementiert worden ist. Dennoch wurde von DANTE ein Plan erstellt mit einfacheren Mitteln ein solchen Root-DSA aufzubauen und zu testen.

In eine solche X.500(93) Infrastruktur soll die LDAP-Welt mit eingebuden werden. Die Tests werden also auch Replikation mit LDAP Servern mit einbeziehen. Eine weitere Integrationsmöglichkeit dieser beiden Directorywelten läßt sich durch das bereits erwähnten DESIRE Indexsystem realisieren. Solange jeder daran beteilgte X.500 Server entweder inhärent oder durch einen vorgeschalteten LDAP Daemon mit einem LDAP Client kommunizieren kann, können die Daten der X.500 Server

[3] siehe http://www.surfnet.nl/surfnet-zoektools/search.html

[4] siehe http://ds.grnet.gr/index_en.html

[5] siehe http://www.desire.org

[6] siehe http://www.opengroup.org

[7] siehe http://www.messagingdirect.com

genauso indiziert werden, wie die der Standalone LDAP Server.

5 Die Situation in Deutschland

In Deutschland hat es durch DFN-Initiativen im X.500 Directory nicht den gleichen Rückwärtstrend gegeben, wie er sich international zeigt. Es gibt eine ganze Reihe von Organisationen, die sehr aktiv und erfolgreich ihre Personendatenbestände im X.500 pflegen, zum Teil schon mit 93er DSAs. Organisationen, denen der Aufwand, eigene DSAs zu betreiben, zu hoch ist, werden durch das AMBIX-Projekt bedient, das für diese die Personendaten in datenschutzrechtlich abgesicherter Weise im X.500 verwaltet und über LDAP Server zur Verfügung stellt [23]. Durch automatische Aktualisierungsmechanismen (z.B. Überprüfung der Email-Adressen durch Anschreiben), sowie durch ein leicht zu handhabendes ASCII-Interface mit denen die Administratoren neue Daten und Datenänderungen liefern können wird die Aktualität des Datenbestandes gewährleistet.

Aber auch in Deutschland sammeln sich unter c=DE viele veraltete Einträge an. Um diesem Problem zu begegnen, müssen Richtlinien für die Qualität von Einträgen aufgestellt werden. Eine Diskussionsgrundlage hierfür liegt vor [24].

Es gibt auch in Deutschland Organisationen, die dem LDAP-Trend folgen und eigene LDAP-Server betreiben. Hierbei handelt es sich nicht nur um White Pages Services, sondern auch andere Directory-Anwendungen wie Public-Key-Verwaltung, Network Information System (NIS) und Directory Enabled Networking (DEN) können mit LDAP realisiert werden.

Das Projekt DFN Directory Services, welches sowohl die AMBIX Arbeit, als auch die Verwaltung des First-Level-DSAs übernommen hat, ist bemüht eine Infrastruktur in Deutschland zu schaffen, die einerseits mit den internationalen Bemühungen kompatibel ist, und andererseits alle beschriebenen Trends in Deutschland integriert. Es geht also darum, eine X.500(93) Infrastruktur aufzubauen, wo ein First-Level-DSA Teil des internationalen Backbones ist und die deutschen X.500 Server der verschiedenen Hersteller, sowie LDAP Server miteinander verbindet.

Das Projekt beteiligt sich aktiv an den Tests des internationalen Backbones, und übernimmt in diesen Tests im Augenblick auch die Verwaltung des Root-DSAs, da sich DANTE wegen Personalmangels im Augenblick nicht an den Tests beteiligen kann. Außerdem unterstützt das Projekt aktiv die Implementierung des DESIRE Index.

In Deutschland wird das Projekt sich bemühen, neue Richtlinien für den Betrieb zu erstellen um eine homogene Integration der verschiedenen Serverlandschaften zu fördern. Um die Replikation zwischen X.500(88), X.500(93) und LDAP zu ermöglichen werden einfache Mechanismen definiert die auf überall vorhandene Technologien, wie FTP und LDAP Data Interchange Format (LDIF) aufbauen. Schließlich wird das Projekt den deutschen Teil des Europäischen Directory Index verwalten.

6 Referenzen

[1] P. Gietz, „Requirements for the future NameFLOW Directory Service“, DANTE in Print 35, [Juli 1998]

[2] M. Wahl, T. Howes, S. Kille, „Lightweight Directory Access Protocol (v3)“, RFC 2251, December 1997

[3] M. Wahl, A. Coulbeck, T. Howes, S. Kille, „Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions“, RFC 2252, December 1997

[4] M. Wahl, S. Kille, T. Howes, „Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names“, RFC 2253, December 1997

[5] B. Blakley, E. Stokes, D. Byrne, P. Behera, „Access Control Requirements for LDAP“, (work in progress) draft-ietf-ldapext-acl-reqts-02.txt, June 1999

[6] B. Blakley, E. Stokes, D. Byrne, „Access Control Model for LDAP“, (work in progress) draft-ietf-ldapext-acl-model-03.txt, June 1999

[7] B. Morgan, Harald Alvestrand, J. Hodges, M. Wahl, „Authentication Methods for LDAP“, (work in progress) draft-ietf-ldapext-authmeth-04.txt, June 1999

[8] E. Stokes, R. Weiser, „LDAP V3 Replication Requirements“, (work in progress) draft-ietf-ldup-replica-req-00.txt, February 1999

[9] E. Reed, U. Srinivasan, John Merrells, „LDAP Replication Architecture“, (work in progress) draft-ietf-ldup-model-01.txt, June 1999

[10] E. Reed, „LDUP Replication Information Model“, (work in progress) draft-ietf-ldup-infomod-00.txt, June 1999

[11] L. Daigle, R. Hedberg, „Technical Infrastructure for Swedish Directory Access Gateways (TISDAG)“, (work in progress) draft-daigle-tisdag-00.txt, June 1999

[12] L. Daigle, T. Eklof, „An Architecture for Integrated Directory Services“, (work in progress) draft-daigle-arch-ids-00.txt, June 1999

[13] T. Eklof, L. Daigle, „Wide Area Directory Deployment Experiences“, (work in progress) draft-eklof-dag-experiences-00.txt, June 1999

[14] H. Alvestrand, R. Hedberg, „Technical Specification - The Norwegian Directory of Directories (NDD)“, (work in progress) draft-hedberg-alvestrand-ndd-00.txt, May 1999

[15] J. Allen, M. Mealling, „The Architecture of the Common Indexing Protocol (CIP)“, RFC 2651, August 1999

[16] J. Allen, M. Mealling, „MIME Object Definitions for the Common Indexing Protocol (CIP)“, RFC 2652, August 1999

[17] J. Allen, P. Leach, R. Hedberg, „ CIP Transport Protocols“, RFC 2653, August 1999

[18] R. Hedberg, B. Greenblatt, R. Moats, M. Wahl, „ A Tagged Index Object for use in the Common Indexing Protocol“, RFC 2654, August 1999

[19] P. Gietz, P. Valkenburg, H. Bekker, „Requirements and overview for an European LDAP indexing service“, (work in progress) draft-gietz-ldapindex-00.txt, June 1999

[20] V. Berkhout, „NameFLOW-Paradise X.500(93) Test Results - Phase One“, DANTE Docs VB(96)15, http://www.dante.net/np/93pilot/phase1-results.html, March 1996

[21] J. Horton, „NameFLOW-Paradise X.500(93) Test Report - Phase two“, DANTE Docs JH(97)001, http://www.dante.net/np/93pilot/phase2-results.html, August 1997.

[22] D. Chadwick, „Managing the X.500 Root Naming Context“, RFC 2120, March 1997

[23] K.P. Gietz, R. Schneider, K. Spanier, „X.500 für alle - Das DFN-Projekt AMBIX“, DFN Mitteilungen 24, November 1996

[24] M. Sauer, „Richtlinien für die Qualität von Einträgen unter c=DE“, (work in progress), August 1999