LDAP GUI-Clients und Client-Schnittstellen

Treffen des ZKI-AK Verzeichnisdienste

Hannover, 24.-25.5.2004

Peter Gietz, DAASI International GmbH

Peter.gietz@daasi.de

DAASI International

Directory Applications for Advanced Security and Information Management

Agenda

- Client-Server-Kommunikation in LDAP
- Konzepte und Architekturen für LDAP-GUIs
- Übersicht Bibliotheken für LDAP-GUIs
- Übersicht LDAP-GUI-Implementierungen
- DSML als neue Schnittstelle für Client GUIs

DAASI International
Directory Applications for Advanced Security and Information Management

Client-Server-Kommunikation in LDAP

- Request-Response Protokoll mit ASN.1 (DER/BER) Encoding
- Jede LDAP-Operation (bind, search, add, modify, modifyDN, delete) unterteilt sich in ein Client-Request und einem Server-Response
- LDAP Operation können durch einen Extension-Mechanismus erweitert werden,
- neue Operationen können ebenfalls spezifiziert werden.
- Viele solche Erweiterungen wurden standardisiert und werden zunehmend in den verschiedenen Produkten implementiert
- Server Response enthält Daten, Verweise, und/oder Error-Codes

DAASI International
Directory Applications for Advanced Security and Information Management

Client-Server-Kommunikation Anforderungen

- Kompatibilität zum LDAPv3-Standard
- einschließlich der vorgeschriebenen Authentifizierungsmechanismen
  - Anonymous bind
  - Simple bind
  - SASL MD5 bind
  - StartTLS
- In manchen EDV-Landschaften ist SASL-GSSAPI-Kerberos5 Mechanismus sinnvoll
- Schema-Unabhängigkeit bei general purpose Clients

DAASI International
Directory Applications for Advanced Security and Information Management

Konzepte und Architekturen für LDAP-GUIs

- Clients, die lokal installiert werden müssen
  - Binaries
  - JavaClients
  - Tcl/Tk
- Gateway Clients
  - Webgateways
  - Web-Services Gateway
  - Weitere XML-Technologien
- Dedizierte Clients
  - PGP
  - X.509
  - Mail User Agents
  - Crawler

DAASI International
Directory Applications for Advanced Security and Information Management

Grundstruktur von LDAP-Clients

- LDAP Bind
- Laden der Server-Information im Root-DSE-Eintrag , z.B.:
  - Welche Extension kennt der Server
  - Welche SASL-Authentifizierung
  - Wo ist der Subschema-Eintrag, in dem das dem Server bekannte Schema veröffentlicht ist
  - Welche Namensräume verwaltet der Server
- Datensuche
- Datenanzeige
- Datenmodifikationen
- LDAP Unbind

DAASI International
Directory Applications for Advanced Security and Information Management

Übersicht Bibliotheken für LDAP-GUIs

- C-Libraries
  - U-Mich, OpenLDAP Clientbibliotheken
  - Netscape, Mozilla SDK
  - IBM SecureWay Directory Client SDK
  - Dedizierte X.509-Zertifikatlibraries
- Java Klassenbibliotheken
  - Novell, OpenLDAP
  - JNDI
- Scriptsprachen LDAP-Bibliotheken
  - PHP
  - Perl
  - Python
- LDAP in Frameworks
  - Zope

DAASI International
Directory Applications for Advanced Security and Information Management

Beispiel für LDAP API

- Funktionen jeweils in synchroner und asynchroner Ausfertigung
- ldap_init() zum Öffnen eine Client-Server-Verbindung
- ldap_bind() zur Authentifizierung mittels verschiedener Mechanismen
- ldap_search() für Suchen
  - Fehler-Codes können mit ldap_result2error() geparsed werden
  - Gefundene Einträge in Schleife abarbeiten mit:
    - ldap_first_entry(), ldap_next_entry()
    - Ldap_first_attribute(),ldap_next_attribute()
- The ldap_unbind() zum Beenden der authentifizierten Session

DAASI International
Directory Applications for Advanced Security and Information Management

Funktionalitäten von LDAP-Clients

- Gute Konfigurierbarkeit
  - Standardparameter (host,port,basedn, etc.)
  - Filter
  - Schema
- Übersichtliche Darstellung der Daten
- Authentifizierung
- Browsen und suchen
- Referrals
- Datenänderungen über Formulare
- Schema-Bewusstheit
- Korrekte Fehlerbehandlung

DAASI International
Directory Applications for Advanced Security and Information Management

Funktionalitäten von LDAP-Clients

- seeAlso
- Paged results
- Serverside-sorting-control
- LDAP Client Udate Protocol (LCUP)
- LDAP Synchronisation
- Entdecken von LDAP-Servern
  - Well known DNS aliases
  - Referrals
  - SRV records
  - Service Location Protocol

DAASI International
Directory Applications for Advanced Security and Information Management

Konfigurierung von LDAP-Clients 1

- Standard-Parameter
  - Hostname
  - Portnummer
  - BaseDN
    - Oberster Knoten des Baumes, ab dem gesucht werden soll
    - Muss nicht Wurzel des Namensraums des Servers sein
  - BindDN Eintrag als der sich der Client authentifizieren soll
  - Bind-Passwort. Passwort dieses Eintrags
  - StartTLS
- Unter Unix können allgemeine LDAP-Client-Parameter für alle Clients in /etc/ldap.conf konfiguriert werden
  - Nicht alle Clients greifen darauf zu!

DAASI International
Directory Applications for Advanced Security and Information Management

Konfigurierung von LDAP-Clients 2

- Konfigurierung, erweiterte Parameter
  - Bind-Methode
  - Zusatzinformationen für alternative Bindmethoden
  - Attribute, die angezeigt werden sollen
  - LDAP-Filter
  - Verhalten bei Referrals
  - Verhalten bei Alias-Einträgen
  - Clientseitige Time- und Size-Limits

DAASI International
Directory Applications for Advanced Security and Information Management

Probleme der Produktübersicht

- Grosse Anzahl von Produkten
- Grosse Fluktuation
  - Firmen werden aufgekauft
  - Allianzen geschnürt
- Test von Verzeichnisdienstprodukten sehr aufwendig
- Performancetests abhängig von Konfiguration
- Ein wirklich guten Überblick zu erstellen ist sehr Zeit- und Kostenaufwendig
- Das hier Gebotene ist also in vielerlei Hinsicht mit Vorsicht zu genießen

DAASI International
Directory Applications for Advanced Security and Information Management

Open Source Software

- + Herstellerunabhängigkeit
- + Grössere Sicherheit:
  - Keine versteckten „Hintertüren“
  - Sicherheitspatches oft schneller entdeckt und behoben
- + Größere Flexibilität
  - Man kann benötigte Features selbst implementieren (lassen)
- + Keine Lizenskosten
- - Roadmaps mancher OpenSource-Projekte werden nicht eingehalten
  - Zur Risiko-Verminderung sollte man zur Not selber am Code arbeiten können
  - Oder Support einkaufen

DAASI International
Directory Applications for Advanced Security and Information Management

LDAP Client Übersicht

- Gute Informationsquelle: www.verzeichnisdienst.de
  - Hauptquelle für die folgende Übersicht
- Viele kostenlose Clients
- Große Auswahl

DAASI International
Directory Applications for Advanced Security and Information Management

Übersicht LDAP-GUI-Implementierungen 1

- Calendra Directory Manager
  - Verzeichnisinhalte graphisch in Organigrammform dargestellt
  - durch Java ein plattform-unabhängig
  - Web-basierten Verzeichniszugriff
  - Abfrage über Mobiltelefon (WML, WAP)
- LDAP Browser/Editor
  - in Java geschrieben
  - Windows-Explorer ähnlichen Interface
  - Windows und Linux
  - Subtree delete
  - Kostenlos
- LinPlanet
  - Administrationstools für LDAP-Server

DAASI International
Directory Applications for Advanced Security and Information Management

Übersicht LDAP-GUI-Implementierungen 2

- Softerra
  - LDAP Browser
    - Win95/98/NT/2000 Browser für LDAPv2 und v3
    - kostenlos
  - LDAP Administrator
    - Win95/98/NT/2000 Administrationstool für LDAPv2 und v3
- Microsoft Active Directory Client Extensions
  - Für Windows 95, 98 und NT Workstation 4.0
  - ADS-Features
  - ADSI, NTLMv2 Authentifizierung und DFS Zugriff
- Cygsoft LDAP Browser
  - Sehr instabil

DAASI International
Directory Applications for Advanced Security and Information Management

Übersicht LDAP-GUI-Implementierungen 3

- DTASI LDAP Browser
  - In Java geschrieben
  - Im Internet Explorer Integriert
- Ernestine
  - LDAP-Client für MacOS
  - Applescript-fähig
- EWI Directory Organization Chart
  - Webbasiert
  - Auf Mitarbeiterverwaltung spezialisiert
  - Organigramm-Funktion
  - Für Windows and UNIX
  - Unterstütz sowohl LDAP als auch RDBMs als Server
  - Workflow Tools.

DAASI International
Directory Applications for Advanced Security and Information Management

Übersicht LDAP-GUI-Implementierungen 4

- Frood
  - Open Source LDAP-Client
  - Perl und GTK
  - Also Plattformunabhängig
- GQ
  - GTK-basierter LDAP-Client
  - Linux, etc.
  - Kostenlos
  - Browsen, Suchen, Datenänderungen
  - Keine neuen Attributtypen ergänzbar
  - Neueste Version unterstützt kein LDAP v2
- Jxplorer
  - Open Source Java
  - Verschieben und Löschen von Teilbäumen
  - UTF8
  - Zertifikat-Darstellung

DAASI International
Directory Applications for Advanced Security and Information Management

Übersicht LDAP-GUI-Implementierungen 5

- KLDAP
  - Open Source C
  - LDAP Client für die KDE-Umgebung
- LDAP aBook
  - freie PERL-/Web-basierte Adressbuch-Anwendung
- LDAP Scout for Eclipse
  - Open Source unter LGPL-Lizenz
  - Speziell für die Eclipse-Umgebung entwickelt
  - LDAP Browser
  - Daten können angezeigt und gelöscht werden
  - Linux, Windows, Solaris, u.a.
- Maxware Directory Explorer
  - LDAP-Client der sich in Explorer integriert

DAASI International
Directory Applications for Advanced Security and Information Management

Übersicht LDAP-GUI-Implementierungen 6

- TWEB
  - C-Webgateway
  - Enthält Sonderfeatures für AMBIX und das elektronische Telefonbuch der Universität Tübingen
- Web2Ldap
  - LDAP-WWW-Webgateway
  - www.stroeder.com
  - In Python geschrieben
  - Sehr gute Zertifikatsdarstellung
  - Sehr gute Schema-Unterstützung
    - Interpretiert Schemaspezifizierung des Servers
- W2l
  - Perl-Webgateway
  - Interpretiert datenschutzrelevante Attribute (AMBIX)
  - Crawlerdetection

DAASI International
Directory Applications for Advanced Security and Information Management

Spezialisierte LDAP-Clients

- Mail User Agents
  - Netscape Communicator LDAP-Adressbücher
  - MS Outlook
- Web-Browser
  - Unterstützung von LDAP-URLs
- Authentifizierungs-Schnittstellen
  - PAM_LDAP
  - NSS_LDAP
- Serververwaltung
  - LDAP basiertes Servermanagement-Tool von Univention
- Bei LDAP Server Produkten werden meistens Clients mitgeliefert

DAASI International
Directory Applications for Advanced Security and Information Management

Schritte vor der Produktwahl

DAASI International

Directory Applications
for Advanced Security
and Information Management

Was ist bei einem LDAP-Projekt zu beachten

- Wie üblich: zuerst Anforderungen analysieren
- Schema Design
  - Zuerst schauen, was für Schemata es schon gibt (Standards verwenden!)
    - In Zukunft einfach bei www.schemareg.org vorbeischauen
  - Sorgfalt bei eigenen Objektklassen und Attributtypen
- Workarounds vermeiden wie
  - Schemacheck off
  - Extensible object
- DIT-Struktur Design
- Spezifizierung der Client-Anwendungen

DAASI International
Directory Applications for Advanced Security and Information Management

Anforderungen

- Nach der Analyse können Anforderungen spezifiziert werden
  - Implementierbarkeit der Datenflüsse
  - Schnittstellen zu Datenbanken spezifizieren
  - Anforderungen an Daten-Management-Funktionalität
  - Anforderung an Datenmengen
  - Anforderungen an Performance

DAASI International
Directory Applications for Advanced Security and Information Management

Erst dann kommt die Produktwahl

- Kriterien:
  - Plattformunterstützung
  - Standardkonformität
  - Leistungsumfang
  - Anpassbarkeit
  - Performance
  - Vorlieben in der eigenen Community
  - Lizenzmodell
  - Sonderkonditionen für Hochschulen
    - Oft nur, wenn mehrere Organisationen gemeinsam beschaffen

DAASI International
Directory Applications for Advanced Security and Information Management

DSML als neue Schnittstelle für Client GUIs

- Directory Service Markup Language
- DSML spezifiziert ein XML-Schema
  - In Version 1 für LDAP-Schema und LDAP Daten
  - In Version 2 für LDAP-Operationen
- DSML wird zunehmend in LDAP-Produkten implementiert (Server und Gateways)
- DSML lässt sich wie jede XML-Sprache relativ einfach mittels XSLT-Skripten in eine andere XML-Sprache konvertieren
- DSML kann eine wichtige Schnittstelle zu intelligenten Web-Services werden
- SPML (Service Provisioning Markup Language) ist kompatibel mit DSML

DAASI International
Directory Applications for Advanced Security and Information Management

DSMLv1 Struktur

```
<dsml:dsml xmlns:dsml="http://www.dsml.org/DSML">
  <!-- a document with both -->
  <dsml:directory-schema>
    <dsml:class id="..." ...>...</dsml:class>
    <dsml:attribute-type id="..." ...>...</dsml:attribute-type>
  </dsml:directory-schema>
  <dsml:directory-entries>
    <dsml:entry dn="...">...</dsml:entry>
   <dsml:entry dn="...">...</dsml:entry>
    <dsml:entry dn="...">...</dsml:entry>
    ...
  </dsml:directory-entries>
 <dsml:dsml>
```

DAASI International
Directory Applications for Advanced Security and Information Management

DSMLv1 Daten

```
<dsml:entry dn="uid=prabbit,ou=development,o=bowstreet,c=us">
  <dsml:objectclass>
    <dsml:oc-value>top</dsml:oc-value>
    <dsml:oc-value>person</dsml:oc-value>
    <dsml:oc-value>organizationalPerson</dsml:oc-value>
    <dsml:oc-value>inetOrgPerson</dsml:oc-value>
  </dsml:objectclass>
  <dsml:attr name="cn"><dsml:value>Peter Rabbit</dsml:value>
  <dsml:attr name="sn"><dsml:value>Rabbit</dsml:value></dsml:attr>
  <dsml:attr name="uid"><dsml:value>prabbit</dsml:value></dsml:attr>
  ....
</dsml:entry>
```

DAASI International
Directory Applications for Advanced Security and Information Management

DSMLv2 Struktur

- Anfrage:

```
<batchRequest xmlns="urn:oasis:names:tc:DSML:2:0:core">
  <modifyRequest>...</modifyRequest>
  <addRequest>...</addRequest>
  <delRequest>...</delRequest>
  <addRequest>...</addRequest>
</batchRequest>
```

- Antwort:

```
<batchResponse xmlns="urn:oasis:names:tc:DSML:2:0:core">
  <modifyResponse>...</modifyResponse>
  <addResponse>...</addResponse>
  <delResponse>...</delResponse>
  <addResponse>...</addResponse>
</batchResponse>
```

DAASI International
Directory Applications for Advanced Security and Information Management

DSMLv2 Modify-Beispiel

- Anfrage:

```
<modifyRequest dn="CN=Bob Rush,OU=Dev,DC=Example,DC=COM">
  <modification name="telephoneNumber" operation="replace">
    <value>536 354 2343</value>
    <value>234 212 4534</value>
  </modification>
  <modification name="sn" operation="replace">
    <value>Rush</value>
  </modification>
</modifyRequest>
```

- Antwort:

```
<modifyResponse>
  <resultCode code="53" descr="unwillingToPerform"/>
  <errorMessage>System Attribute may not be modified</errorMessage>
</modifyResponse>
```

DAASI International
Directory Applications for Advanced Security and Information Management

Vielen Dank für Ihre Aufmerksamkeit!

- Noch Fragen?

- DAASI International GmbH
  - Web:www.daasi.de
  - Mail: Info@daasi.de

DAASI International
Directory Applications for Advanced Security and Information Management