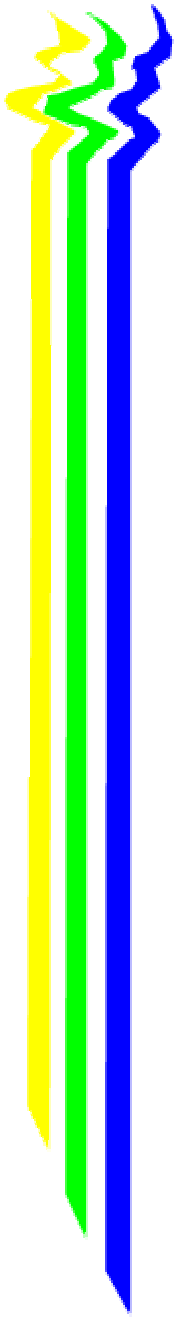
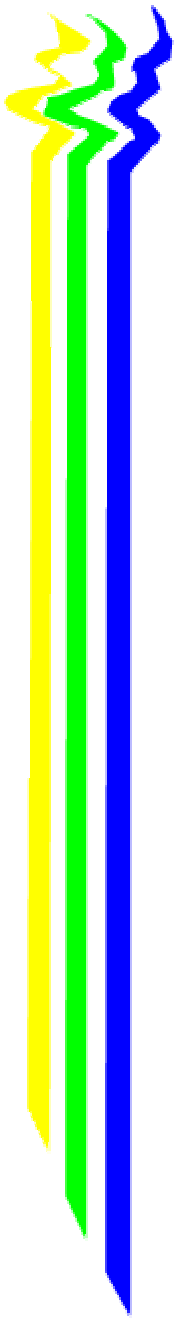


Neue Entwicklungen bei LDAP

Vortrag beim Directory Forum
der 32. DFN-Betriebstagung
am 23.3.2000 in Berlin

Peter Gietz
DFN Directory Services
peter.gietz@directory.dfn.de

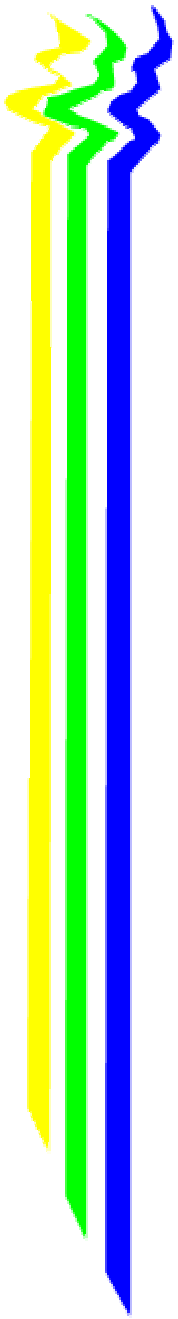


Agenda

- LDAP Core und Erweiterungsmöglichkeiten
- neuere Ldapext-RFCs
- neuere Ldapext-Drafts
- Andere IETF WGs mit LDAP Drafts
- Access Control
- Authentifizierung
- [LDAP und DEN]

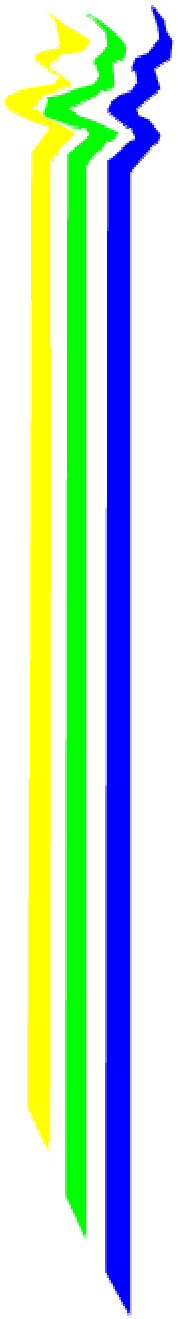
LDAP Core

- Lightweight Directory Access Protocol
- Aktuelle Version 3
- IETF-Standard (RFC 2251-2256)
- Nicht nur Access Protocol, sondern wie X.500 vollständiges Client-Server-System
- Alle Directory-Implementierungen haben LDAP-Schnittstelle (X.500, Novell NDS, MS AD)
- Viele Clientaplikationen haben LDAP-Schnittstelle (z.B. Mailprogramme, Browser)



LDAP Operationen

- Abfrage:
  - search
  - compare
- Datenänderung:
  - add
  - delete
  - modify
  - modifyDN
- Authentifizierung und Kontrolle:
  - bind
  - unbind
  - abandon

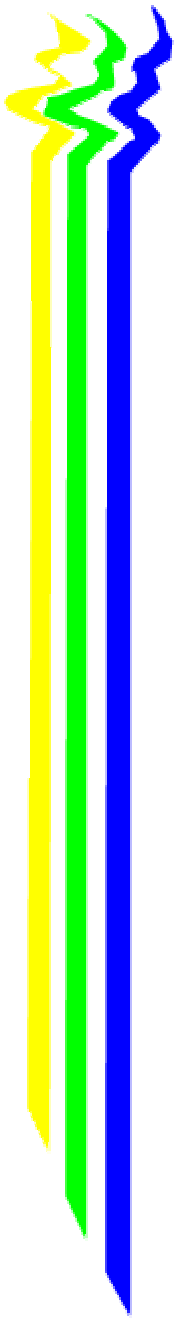


LDAP v3 Erweiterungen

- LDAP extended operations (RFC 2251, 4.12)
  - neue Protokoll-Operation (zusätzlich zu den 9 in RFC 2251 definierten), z.B. StartTLS Operation
  - ExtendedRequest: requestName, [requestValue]
  - ExtendedResponse: LDAPResult,[responseName, response]
- LDAP controls (RFC 2251, 4.1.12)
  - zusätzliche Information für die 9 Standard-operationen, die deren Verhalten modifizieren
  - Control: controlType, criticality, [controlValue]
- SASL Mechanismen
  - Simple Authentication and Security Layer
  - Rahmen zur Unterstützung verschiedener Authentifizierungsmechanismen

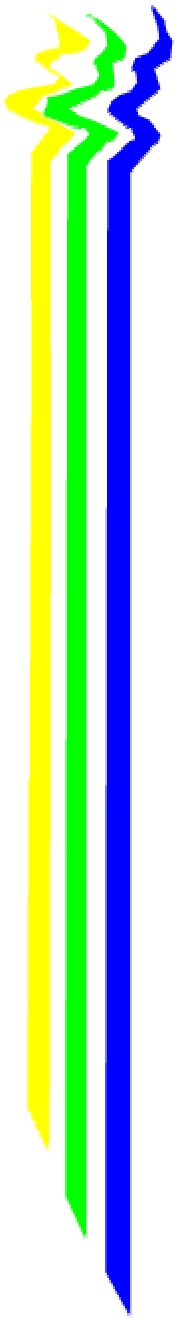
LDAPv3 Erweiterungen (2)

- Erweiterungen werden in IETF-ldapext standardisiert
  - Vertreter von Netscape, Innosoft, Microsoft und Novell sehr aktiv



LDAPv3 Erweiterungen (3)

- Root DSE Eintrag
  - Spezieller Eintrag im LDAP-Server
  - Enthält Attribute, die beschreiben, welche LDAP-Erweiterungen vom Server unterstützt werden:
    - namingContext
    - subschemaSubentry
    - altServer
    - supportedExtensions
    - supportedControl
    - supportedSASLMechanism
    - supportedLDAPVersion

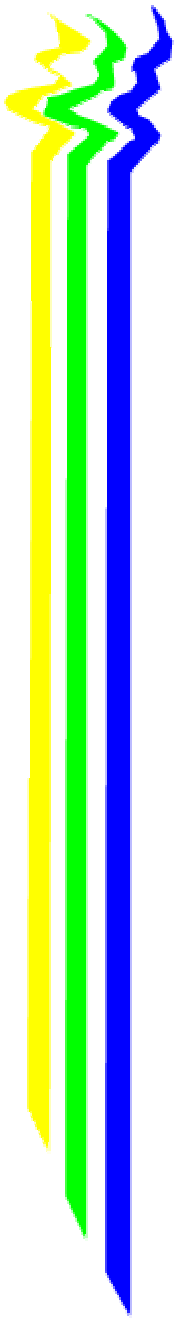


Neuere LDAPext RFCs

- RFC 2589
- RFC 2596
- RFC 2649
- RFC 2696

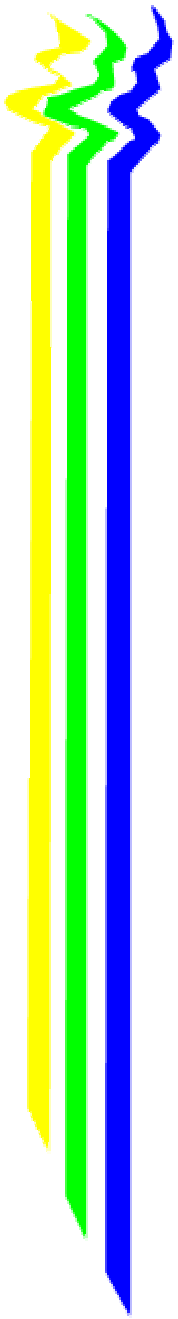
RFC 2589

- Yaacovi, Y (MS); Wahl, M. (Innosoft), Genovese, T. (MS): LDAPv3: Extensions for Dynamic Directory Services, May 1999 (Standards Track)
  - Dynamische Einträge im Directory
  - Periodisches Auffrischen der Information
  - z.B. für Online-Status-Information, bei Video Konferenzen
  - Definiert:
    - Client und Server Requirements
    - ExtendedRequest (refresh request)
    - ExtendedResponse (refresh response)
    - OC dynamicObject mit Attr. EntryTt1 (Anzahl Sekunden)



RFC 2596

- Wahl, M. (Innosoft), Howes, T. (Netscape), Use of Language Codes in LDAP, May 1999 (Standards Track)
  - Sprachidentifizierende Tags nach RFC 1766
  - Format: <Attrib>; lang-<Sprachcode>
  - Beispiel: givenName; lang-en-US
  - Darf nicht im DN verwendet werden
  - Darf verwendet werden in:
    - Suchfilter, z.B.:
      ldap: //host:389/c=de??(cn;lang-en=X*)
    - Compare request
    - requested Attribute, z.B.:
      ldap: //host:389/c=de?cn;lang-en?(objectclass=*)
    - Add Operation
    - Modify Operation

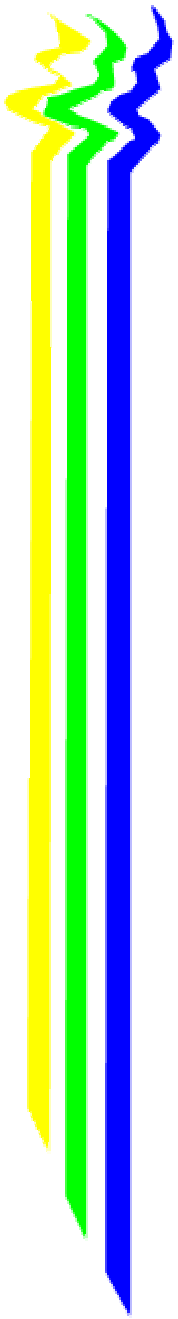


RFC 2649

- Greenblatt, B., Richard, P.: An LDAP Control and Schema for Holding Operation Signatures, August 1999 (Experimental)
  - Client schickt Änderung eines Eintrags auf gesichertem Wege (z.B. TLS) und signiert diese Änderung mit S/MIME Technologie, oder läßt sie vom Server signieren
  - Komplettes Journal der Veränderungen eines Eintrags
  - Definiert:
    - Control SignedOperation
    - Control DemandSignedResult
    - Control SignedResult
    - OC signedAuditTrail mit Attr Changes
    - OC zombieObject mit Attr Changes u. OriginalObject
    - RootDSE-Attr signedDirectoryOperationSupport

RFC 2696

- Weider, C., Herron, A., Anantha, A (MS), Howes, T. (Netscape): LDAP Control Extension for Simple Paged Results Manipulation, September 1999 (Informational)
  - Mechanismus durch den der Server mehrere Teilmengen als Ergebnis zurückgeben kann
  - Client definiert wieviele Einträge pro Page
  - Definiert:
    - Control pagedResultsControl
    - searchControlValue: realSearchControlValue
      - size (Anzahl der Einträge)
      - cookie (zur Reidentifizierung des Suchauftrags)



Aktuelle LDAPext Drafts

- Drafts zu Acces Control und Authentifizierung
  - TLS extensions, X.509 Auth mit SASL
- Drafts zu Client-Server Kommunikation
  - serverside sorting, virtual lists, persistant search, Referrals, matched values
- Drafts zu APIs
  - C-API und extensions, Java-API und extensions, zusätzliche Fehlercodes, etc.
- Zahllose Indivual Submissions, z.B.:
  - LDIF, client update, MS AD, Novell NDS

LDAP Drafts andere IETF WGs

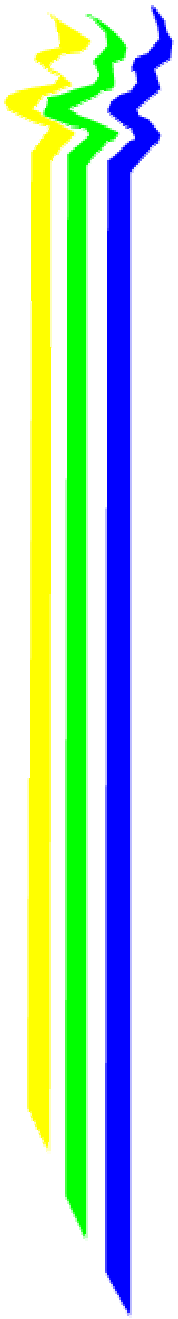
- LDUP
  - LDAP Duplication/Replication/Update Protocols
- Policy
  - Policy Framework
  - DEN (Directory Enabled Networking)
  - QoS (Quality of Service)
- PKIX
  - Public Key Infrastructure (X.509)
- Calsch
  - Calendering and Scheduling

Access Control Requirements

- Stokes, E., Byrne, D. (IBM), Blakey, B. (Dascom), Behera, P. (Netscape): Access Control Requirements for LDAP, <draft-ietf-ldapext-acl-reqts-03.txt>, February 2000
  - Anforderungen an Access Control Lists für LDAP:
  - Einfach und hocheffizient, erweiterbar
  - spezifischere Policies überschreiben unspezifischere
  - Default Policy für Neueinträge
  - Reihenfolge der Einträge in ACL irrelevant
  - Alle ACLs explizit
  - Eine Policy für mehrere verstreute Einträge
  - ...

Access Control Model (1)

- Stokes, E., Byrne, D. (IBM), Blakey, B. (Dascom): Access Control Model for LDAP, <draft-ietf-ldapext-acl-model-05.txt>, March 2000
  - LDAP Funktionsmodell (add, delete, modify und search) zur Manipulation von Access Control Information
  - Zusätzliches Controls:
    - getEffectiveRightsRequest und -Response
  - Root DSE Attribut supportedACIMechanism mit Attribut aCIMechanism
  - Rechte für Attribute: Read, Write, Search, Compare
  - Rechte für Einträge: Add, Delete, EditDN, BrowseDN
  - Versch. DN-Typen: access-id, group, role, (ip-Address, kerberosID)
  - policyOwner Attribut, bestimmt wer ACIs setzen darf

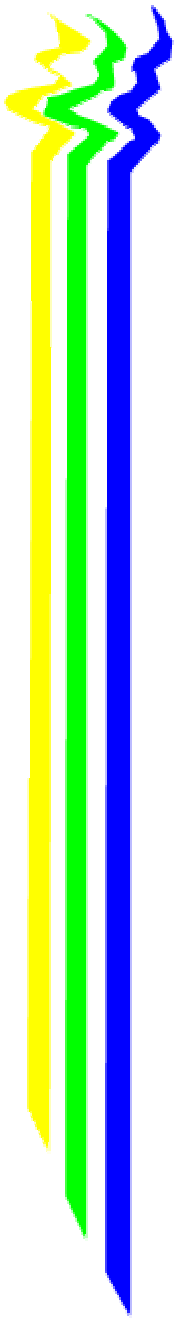


Access Control Model (2)

- Basic ACI Attribute ldapACI
  - Speichert die AC Information:
    - OID
    - scope (entry / subtree)
    - rights (grant / deny)
      - grant; <permission>; <Attribute>
      - permissions: a, d, r, s, w, c, e, b
      - Attribute: »collection«, »all«, »entry«
    - dnType (accessid / group / role, ...)
    - subjectDN (DN / »public« / »this«)

Access Control Modell (3)

- Beispiele:
  - Ein User wird als PolicyOwner definiert:
    policyOwner: 1.2.3#subtree#access-id#cn=Spanier
  - *Eine Gruppe darf bestimmtes Attribut im Subtree lesen, suchen oder vergleichen:*
    ldapACI: 1.2.3#subtree#grant;r,s,c;attribute:attr1#
    group#cn=Dept XYZ, c=US
  - *Eine Roleoccupant darf im Subtree Einträge anlegen und Attribute 2 und 3 lesen, suchen und vergleichen:*
    ldapACI: 1.2.3#subtree#grant;a;collection:[entry]#
    role#cn=SysAdmins,o=Company
    ldapACI: 1.2.3#subtree#grant;r,s,c;attribute:attr2#
    role#cn=SysAdmins,o=Company
    ldapACI: 1.2.3#subtree#grant;r,s,c;attribute:attr3#
    role#cn=SysAdmins,o=Company



Authentication Methods (1)

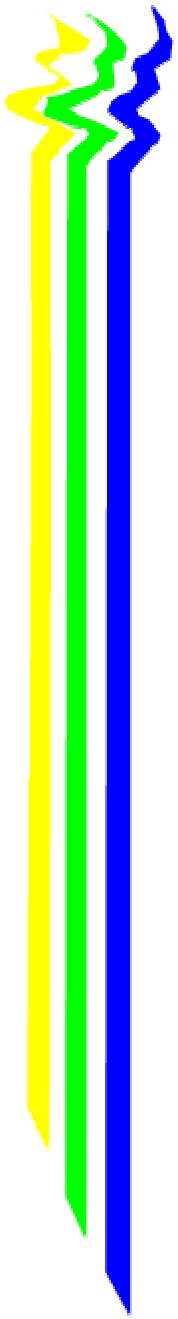
- Wahl, M. (Innosoft), Alvestrand, H. (MaxWare), Hodges, J. (Stanford Univ.), Morgan, RL. (Stanford Univ.), Authentication Methods for LDAP, <draft-ietf-ldapext-authmeth-04.txt>, June 1999
  - Begriffsbestimmungen
    - Access Control Policy, z.B. ACL
    - Access Control Factor (ACF), z.B.:
      - Authentifizierte Identität
      - Source IP Adresse
      - Stärke der Verschlüsselung
      - gewünschte Operation
      - Tageszeit
      - ...
    - Operation x auf Resource Y bei ACFs a,b,c

Authentication Methods (2)

- Authentifizierung:
  - Prozess der Erzeugung, Übertragung, Verifizierung von Berechtigungen durch Beglaubigung von Identität
- Authentifizierungsmethoden:
  - Definition von Kombinationen von Security-Mechanismen

Authentication Methods (3)

- Profiles
  - (1) öffentlicher read-only Server:
    - anonyme Authentifizierung
  - (2) Server mit Passwortgestützte Authentifizierung:
    - Passwortübertragung muß verschlüsselt sein
    - Digest-MD5 SASL Mechanismus <draft-leach-digest-sasl-00.txt>



Authentification Methods (4)

- (3) Server mit Gesamtverbindungsschutz:
  - Start TLS Extended Operation (Verschlüsselung der gesamten Verbindung)
  - und Einfache Authentifizierung (simple bind)
  - oder Authentifizierung mit SASL External Mechanismus (-> RFC 2222)
  - zusätzlich möglich (SHOULD): Zertifikats gestützte Authentifizierung mit TLS

Authentication Response Control

- Weltman, R. (Nestcape), Smith, M. (Netscape), LDAP Authentication Response Controll, <draft-weltman-ldapv3-auth-response-01.txt>, Februar 2000
  - Server gibt Zusatzinformation beim Bind-Response zurück
  - AuthResponseControl:
    - OID, FALSE, AuthResponseValue
  - AuthResponseValue:
    - authDN
    - authMechanism