univention
linux for your business

Samba und OpenLDAP in der Oldenburgischen Landesbank

Samba eXPerience 2004,
7.4.2004

Peter H. Ganten
Geschäftsführer
ganten@univention.de

Agenda

- Vorstellung Univention GmbH
  - Mission, Kompetenzen, Produkte, Kunden
- Ausgangssituation bei der OLB
  - Aufstellung der OLB, IT-Infrastruktur, Herausforderungen
- Projektziele
- Konzept und Roll-Out einer erneuerten Infrastruktur
  - LDAP (Aufbau, Replikation, Rechteverwaltung, ...)
  - Samba (Konfiguration, Probleme)
- Status, Zusammenfassung und Diskussion

univention
linux for your business

Agenda

- Vorstellung Univention GmbH
  - Mission, Kompetenzen, Produkte, Kunden
- Ausgangssituation bei der OLB
  - Aufstellung der OLB, IT-Infrastruktur, Herausforderungen
- Projektziele
- Konzept und Roll-Out einer erneuerten Infrastruktur
  - LDAP (Aufbau, Replikation, Rechteverwaltung, ...)
  - Samba (Konfiguration, Probleme)
- Status, Zusammenfassung und Diskussion

univention
linux for your business

Mission der Univention GmbH

„Unternehmen und Behörden durch passende Produkte und Dienstleistungen dabei zu unterstützen, Linux-Infrastrukturen erfolgreich einzuführen und auszubauen.„

Kernkompetenzen

- Linux-Implementierung
- Management und Roll-Out komplexer Linux-Infrastrukturen
- Verzeichnisdienste
- Migration von Windows nach Linux
- Integration von Windows und Linux
- Linux als Desktop- und Client-Betriebssystem / Thin-Clients

univention
linux for your business

Univention Corporate Server

- Linux-Distribution auf Basis von Debian GNU/Linux mit Support und Wartung
- Managementsystem auf der Basis von OpenLDAP, Kerberos und DNS
  - Kernkomponenten: Management-Interface (Web, CUI), Event-Notification, Policy-basierte Administration
- Module u.a. für Thin Client Infrastruktur, Mail, Fax, Services for Windows u.a.

Kunden (1)

- Public Sector:
  - Senator für Finanzen, Bremen
  - Senator für Bildung und Wissenschaft, Bremen
  - Bundesamt für Sicherheit in der Informationstechnologie
  - Bundesbeschaffungsamt
  - Bundesinnenministerium,
  - Bundeskartellamt
  - Landesbetrieb für Datenverarbeitung und Statistik, Brandenburg

Bundesamt für Sicherheit in der Informationstechnik

Bundesministerium des Innern

Kunden (2)

- Private Sector
  - BWG Reimer, Bremen
  - Flamme Gruppe, Bremen
  - Friedhelm Loh Gruppe
  - MKG Bank (Mitsubishi), Frankfurt
  - Oldenburgische Landesbank
  - Stahlberg-Roensch, Seevetal

univention
linux for your business

Weitere Informationen

- Langsam wachsendes Unternehmen
- Zur Zeit 12 feste und mehrere freie Mitarbeiter
- Seit der Gründung (02/2002) profitabel
- Kein Fremdkapital / keine fremden Beteiligungen
- http://www.univention.de/

univention
linux for your business

Agenda

- Vorstellung Univention GmbH
  - Mission, Kompetenzen, Produkte, Kunden
- Ausgangssituation bei der OLB
  - Aufstellung der OLB, IT-Infrastruktur, Herausforderungen
- Projektziele
- Konzept und Roll-Out einer erneuerten Infrastruktur
  - LDAP (Aufbau, Replikation, Rechteverwaltung, ...)
  - Samba (Konfiguration, Probleme)
- Status, Zusammenfassung und Diskussion

Die Oldenburgische Landesbank (OLB)

- Führende Regionalbank in der Weser-Ems-Region
- Zentrale in Oldenburg
- Filialbank mit Geschäfts- und Firmenkunden
- ca. 30 Filialen und 170 Geschäftsstellen
- ca. 2000 Mitarbeiter

Oldenburgische Landesbank

Ausgangssituation

- Zentrale Benutzerdatenbank (TEO, Oracle)
- Zentrale: SUN-Server mit PC Netlink
- Filialen und Geschäftsstellen: Server mit SuSE 5.2, Kernel 2.0, Samba 2.2.x
- 64 kBit Leitungen für Geschäftsstellen
- Skript-basierter Account-Abgleich aus TEO
- Clients: MS Windows NT 4.0

Herausforderungen

- Softwareaktualisierungen
- Abweichende Domänen-SIDs
- Keine einheitlichen UIDs, GIDs und SIDs
- Passwortänderungen durch Benutzer
- Passwort-Policies und -History
- Domänengruppen
- Client Migration nach Windows XP
- Single Source of Authentication

univention
linux for your business

Agenda

- Vorstellung Univention GmbH
  - Mission, Kompetenzen, Produkte, Kunden
- Ausgangssituation bei der OLB
  - Aufstellung der OLB, IT-Infrastruktur, Herausforderungen
- Projektziele
- Konzept und Roll-Out einer erneuerten Infrastruktur
  - LDAP (Aufbau, Replikation, Rechteverwaltung, ...)
  - Samba (Konfiguration, Probleme)
- Status, Zusammenfassung und Diskussion

Projektziele (1)

- Modernisierung der Software
  - File- und Directory-ACLs
  - Domänegruppen
- Verbesserung der Passwort-Verwaltung
  - Passwort-Policies, verschl. Passwörter
  - Änderung durch Benutzer und spez. Accounts
- Einheitlicher GID-, UID- und SID-Raum
- Möglichkeit zur Bereitstellung zentr. Shares

Projektziele (2)

- Single-Point-of-Administration (TEO, LDAP)
  - Auch Computerverwaltung incl. DNS und DHCP
- Installations- und Aktualisierungsverfahren
  - Vollautomatische Einrichtung von Servern
  - Einfache Aktualisierung
  - Automatische Installation von Windows-PCs
- Verw. von Root-Accounts einschränken
- Langfr. auch Linux Clients ermöglichen
- Unabhängigkeit vom Netzwerk

univention
linux for your business

Agenda

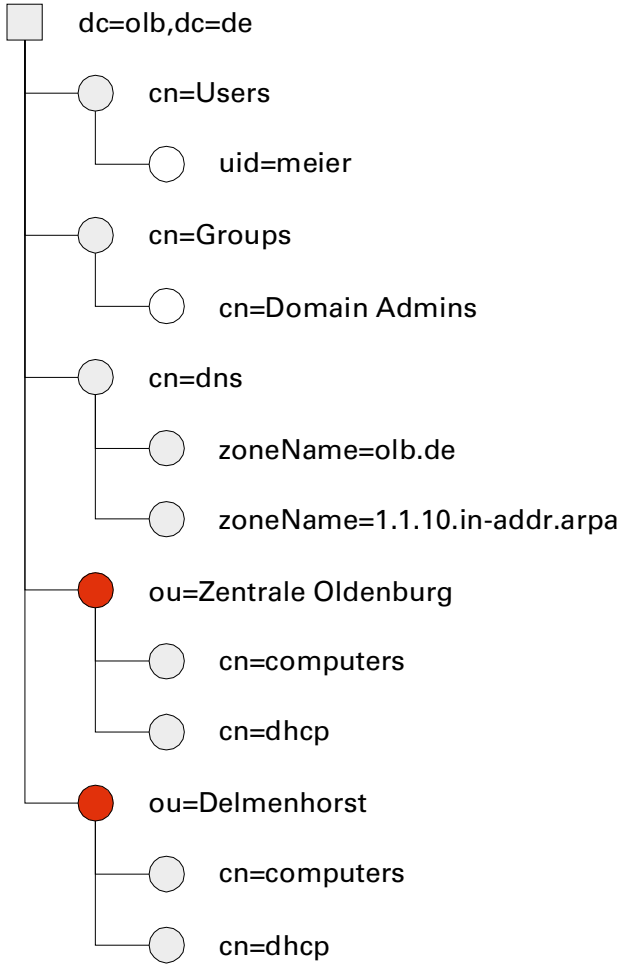
- Vorstellung Univention GmbH
  - Mission, Kompetenzen, Produkte, Kunden
- Ausgangssituation bei der OLB
  - Aufstellung der OLB, IT-Infrastruktur, Herausforderungen
- Projektziele
- Konzept und Roll-Out einer erneuerten Infrastruktur
  - LDAP (Aufbau, Replikation, Rechteverwaltung, ...)
  - Samba (Konfiguration, Probleme)
- Status, Zusammenfassung und Diskussion

OpenLDAP als zentrales Repository

- Verwaltung aller dynamischen Informationen im LDAP:
  - Benutzer, Gruppen
  - Shares, Drucker
  - Computer (incl. DHCP, DNS und Installations-Informationen)
- Skript-basierter Abgleich mit TEO

Directory Information Tree

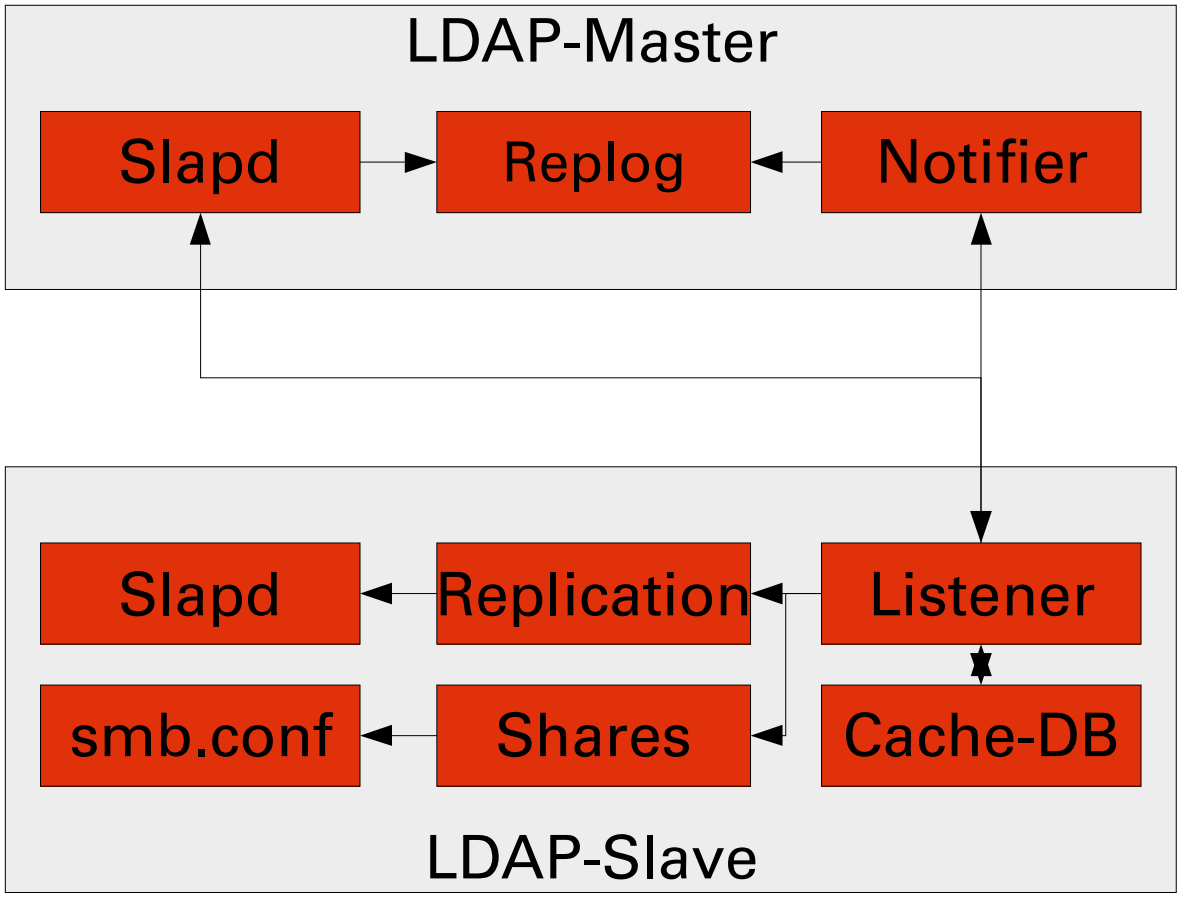
- Basis-DN: dc=olb,dc=de
- Benutzer, Gruppen und DNS unterhalb des Basis-DNs
- Client-PCs und DHCP zu den Filialbereichen
- Zuordnung von Benutzern zu einer oder mehreren Filialen über LDAP-Attribut



LDAP-Replikation (1)

- LDAP-Datenbank an jedem Standort
- Selektive Replikation (ACL-basiert)
- Slurpd-Replikation problematisch
- Deswegen: Eigenes Replikationsverfahren
  - Steuerung über LDAP-ACLs auf dem Master
  - Erlaubt die Verwaltung von Konfigurationen im LDAP-Verzeichnis (z.B. Shares, Drucker)

LDAP-Replikation (2)



LDAP Access Control Lists (ACLs)

- Globale Administratoren-Gruppe
- Passwort-Änderung durch Filial-Admins
- Eigener Bind-DN für jeden Samba-DC
- Samba-Server dürfen Passwörter „ihrer“ Filiale ändern und Benutzer „ihrer“ Filiale lesen
- Benutzer ändern Passwörter über Windows und PAM (Kerberos)

Samba-Konfiguration

- Zur Zeit: Samba 3.0.2a
- PDC / BDC, Member in der Zentrale
- PDC, WINS-Server an den Standorten
- An einigen Standorten zweite Samba-Instanz auf zweitem Netzwerk-Interface
- Konfiguration der XP-Oberfläche über Systempolicies (anderes Projekt)

Passwort-Policies

- Samba- / Windows-Policies reichen nicht
- Realisierung über cracklib und eigenen Quality-Checker
- Passwort-History über Kerberos Quality Checker Modul

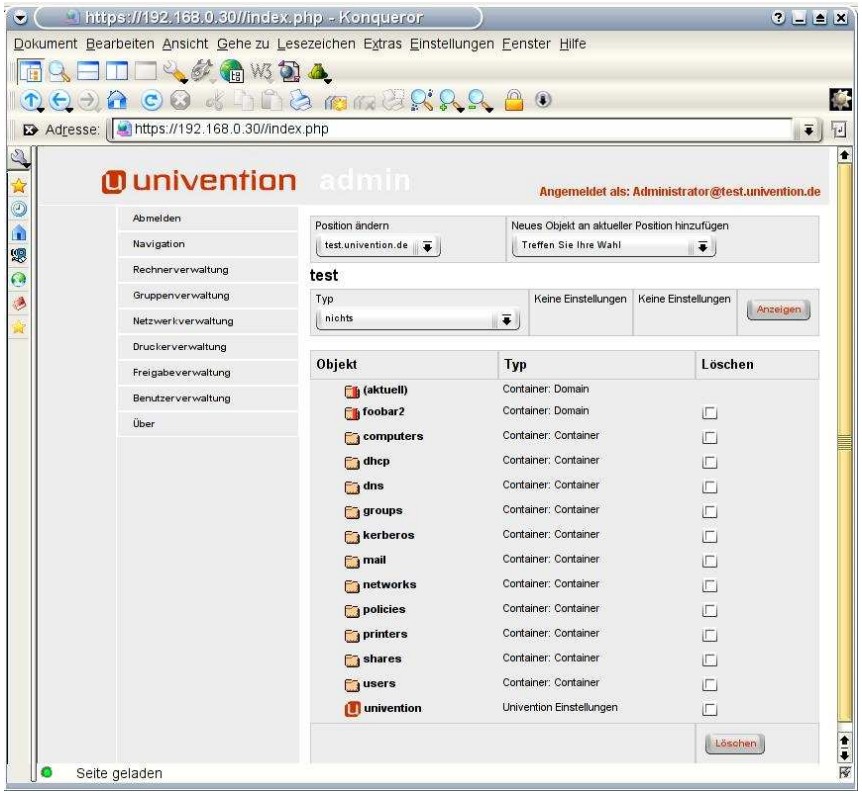
Client-Installation

- Basiert auf Sourceforge-Project unattended
- PXE-Konfiguration über LDAP
- Zuweisung von Installationsprofilen (unattend.txt) über LDAP-Policies

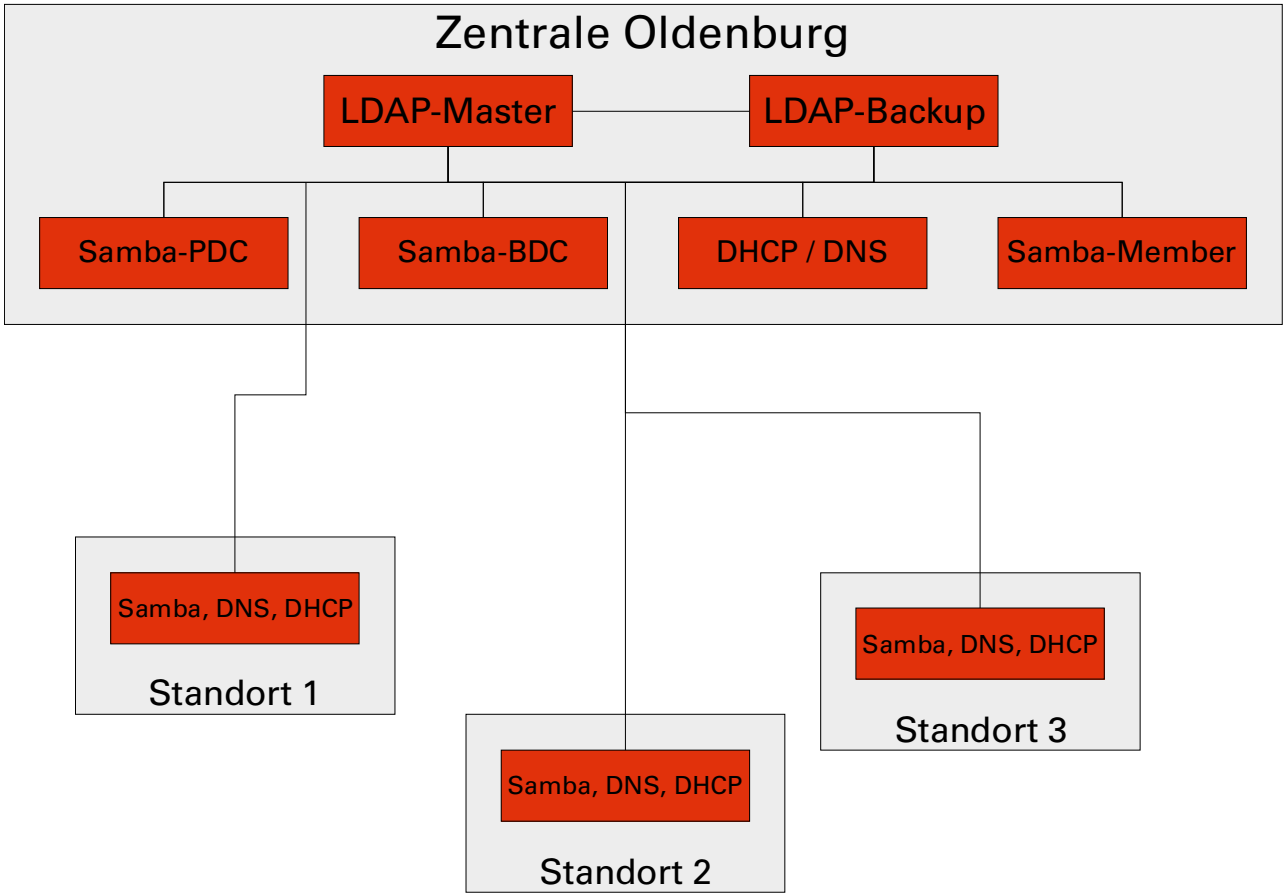
univention
linux for your business

Administration

- Web-basiertes Frontend
- CLI-Frontend zur Automatisierung
- Script-basierter Datenabgleich



Gesamtaufbau



Rollout

- UCS-Installations-CDROM mit Profilen für alle Server (Passwortgeschützt!)
- Einrichtung von LDAP-Master und -Slave
- Automatisches „Joinen“ der Standortserver
- Skript-basierte Migration der Benutzerdaten (UIDs und GIDs)
- Neu-Joinen der Clients unvermeidbar

univention
linux for your business

Agenda

- Vorstellung Univention GmbH
  - Mission, Kompetenzen, Produkte, Kunden
- Ausgangssituation bei der OLB
  - Aufstellung der OLB, IT-Infrastruktur, Herausforderungen
- Projektziele
- Konzept und Roll-Out einer erneuerten Infrastruktur
  - LDAP (Aufbau, Replikation, Rechteverwaltung, ...)
  - Samba (Konfiguration, Probleme)
- Status, Zusammenfassung und Diskussion

Status

- Projekt befindet sich im Roll-Out (Abschluss Ende 2004)
- Weitere Anwendungen und Dienste werden zur Zeit an das Verzeichnis angebunden

Probleme

- OpenLDAP-Performance bei komplexen ACLs
- Timeouts (samba replication sleep, passwd chat timeout)
- Integration Solaris (OpenLDAP Patch)
- Root-User bei Domänen-Joins immer noch erforderlich :-(

Zusammenfassung

- Samba und OpenLDAP sind eine kostengünstige und flexible Alternative zu anderen Lösungen (AD, Novell ...)
- LDAP lässt sich zu einem zentralen Repository für Systemkonfigurationen ausbauen
- Samba 3.0.2a hat sich prinzipiell als unproblematisch erwiesen

univention
linux for your business

Herzlichen Dank für Ihre Aufmerksamkeit!

Mehr Informationen:

Peter Ganten

ganten@univention.de

http://www.univention.de