Hasso Plattner Institut

IT Systems Engineering | Universität Potsdam

Samba4 / Active Directory

Seminar Betriebsystemadministration

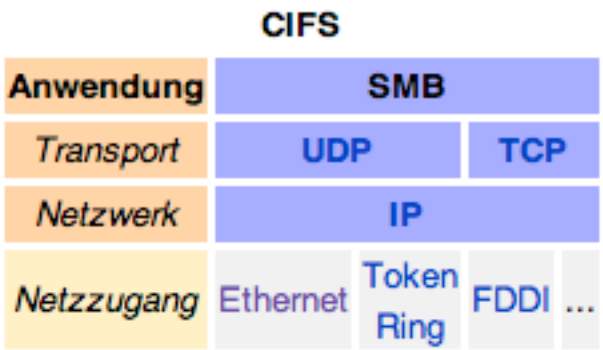
Martin Faust
Hasso-Plattner-Institut Potsdam
Mai 2008

Themen

- Samba
  - SMB Protokoll
  - Aktueller Entwicklungsstand, Ziele
- Active Directory
  - Funktionsweise
  - Installation
  - SRV Resource Records
- Diskussion
  - Einsatz von “Nachbauten” in unternehmenskritischen Bereichen

Server Message Block

- Auch bekannt als CIFS, LAN-Manager- bzw. NetBIOS-Protokoll
- Kommunikationsprotokoll
  - Windows Produktfamilie
  - LAN-Server von IBM
- Anwendungsschicht
  - früher mit NetBIOS & NetBEUI
  - heute direkt über TCP/UDP
- Oft auch für Linux/Unix Dateifreigaben



Samba

- OpenSource Implementierung von SMB
- Aktuell: Samba 3.0.29
  - ausgereifte Datei- und Druckfreigabedienste
  - oft auf SOHO-Nas Geräten installiert
  - kann NT4 PDC ersetzen
  - Mitglied in ActiveDirectoy Domäne
  - AD ähnliches Replizieren mit LDAP Server

Samba4: Aktueller Stand

- bisher einige TP, 3 Alpha Releases
- Fertigstellung: “when it’s done”, eventuell 2009
- Wichtigstes Ziel: ActiveDirectory Domänencontroller
- Installation:
  - git-repository clonen
  - configure , make, make install
  - $PATH anpassen
  - initiale ActiveDirectory Datenbank erstellen lassen
  - bind einrichten
  - smbd starten

Samba4

- Umsetzung von NT-ACLs auf UNIX-ACLS, Alternate Data Streams
  - xattr z.B. in ext3
  - ADS in seperater Datei/Verzeichnis

Derzeitiger Status

- SWAT Webinterface deaktiviert
- Druckdienste nicht implementiert
- Verschiedene Fehler je nach aktuellem Checkout
- Installation nicht zuverlässig beschrieben
- Nach jedem Build erneutes “Provisioning”

Active Directory

- Eingeführt mit Windows 2000 Server
  - Mischbetrieb von Server 2000,2003,2008 möglich
- Nutzen
  - Mehrere Standorte
  - Automatisches Replizieren
  - Zentrale Nutzerverwaltung
  - Gruppenrichtlinien
  - Servergespeicherte Nutzerprofile
- Nachteile
  - Lizenzkosten
- Neuerungen in Server 2008
  - Readonly-DC

Active Directory: Aufbau

Sammlung von Bäumen von Bäumen

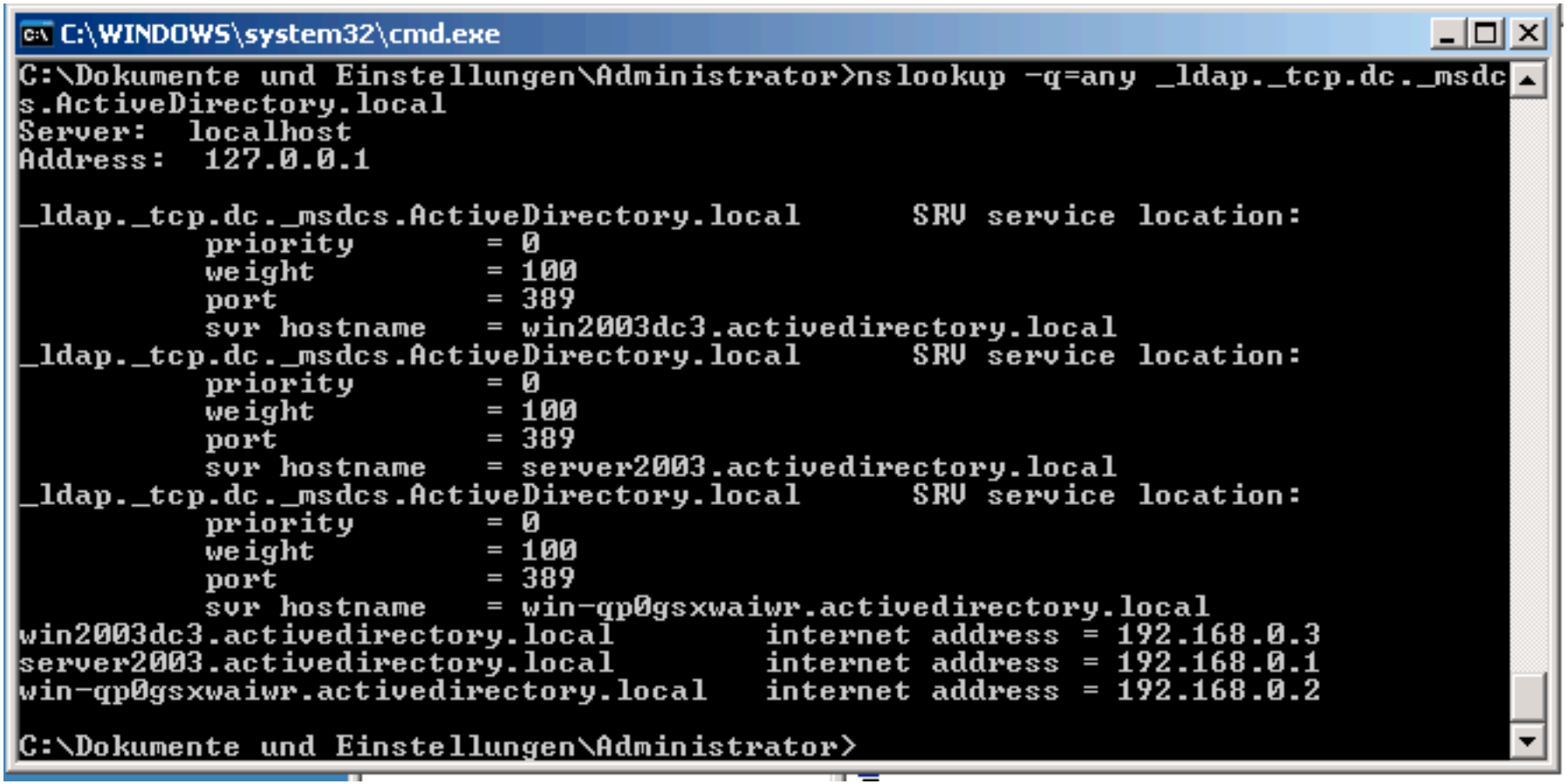
- Gesamtstruktur
  - meist gleich der Struktur
  - hilfreich bei nachträglichen Zusammenschlüssen
- Struktur
  - Domänenbaum
- Domäne
- Organisationseinheiten
  - Gruppen
  - kann weitere OUs enthalten
- Objekte
  - Benutzer, Computer, Drucker

SRV Resource Record

- Dienste im Netz identifizieren
- Aufbau:
  - Service
    - _ldap._tcp.dc.ActiveDirectory.local
  - TTL
  - IN
  - SRV
  - Priorität
  - Gewicht
  - Port
  - Server

Demo

nslookup fuer LDAP-Controller



Kerberos

- Single-Sign Login
- Nutzer erhält Ticket Granting Ticket (TGT)
  - z.B. bei Anmeldung an Workstation
- Mit TGT können Tickets für speziellen Dienst angefordert werden
- TGT gilt für Domäne, weitere Dienste über Vertrauensstellungen

Installation

- Server:
  - Windows Server Grundinstallation
  - IP-Adresse festlegen
  - dcpromo ausführen
    - Erster DC
      - » Grundeinstellungen fuer Domäne
      - » DNS, DHCP
    - Zusätzlicher DC
      - » Domäne angeben, Rest passiert von allein
- Client:
  - Grundinstallation Betriebssystem
  - Domänenmitgliedschaft konfigurieren

Replikation

- Replikation ist Einstellungssache
  - pro Verbindung festlegbar
  - Kostenfaktor für Leitungen
  - auch langes Replikationsintervall oft kein Problem
    - Warum?
      - » Angemeldete Nutzer haben TGT
      - » Neuer Benutzer kann am Standort erzeugt werden wo er gebraucht wird
      - » Passwortänderungen sind am aktuellen Standort sofort verfügbar

Verwaltung

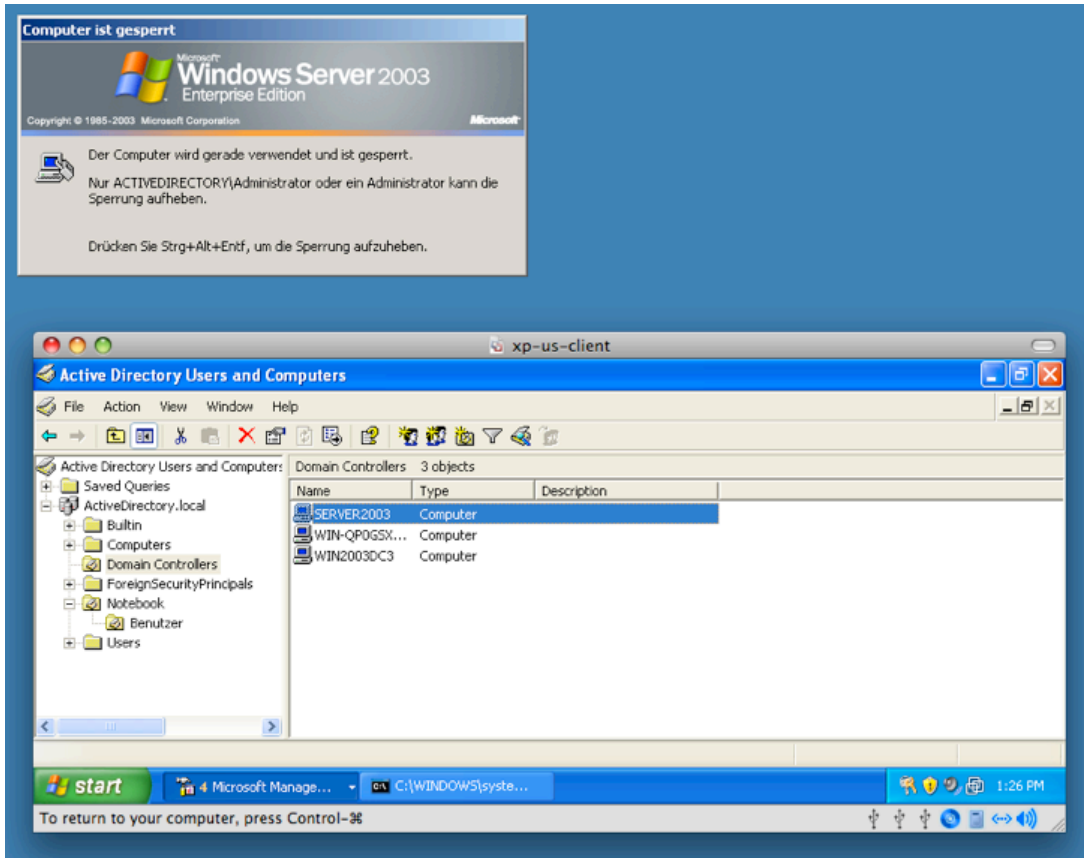
- Microsofts Managementkonsole
  - Die gleichen Tools fuer lokale & entferne Bearbeitung
  - Vollständig verwaltbar von Client-PC, ohne Komforteinbussen
- Snap-Ins für alle AD Verwaltungsaufgaben
  - DNS
  - DHCP
  - Benutzer & Computer
  - ...

Gruppenrichtlinien

- Einstellungen für Benutzer und Computer
- Viele vorgefertigte Einstellungen für Windowsclients
- Einfaches Anwenden von Regeln für gesamtes Unternehmen
- 3 Möglichkeiten je Einstellung: Aktiv, Deaktiviert, nicht konfiguriert
  - Spezifischere Regeln überschreiben globale
  - Lokale Richtlinie findet am Schluss Anwendung

Demo

Verwaltungsmöglichkeiten, Replizierung.



Wo Windows unverzichtbar bleibt

(bei Windows Client-Rechnern)

- WSUS
  - Windows Software Update Services
  - Zentrale Bereitstellung von Updates im Firmennetzwerk
  - Unterstüzt Computergruppen
  - Zurückhalten von Aktualisierungen
  - Schont Bandbreite
- Windows Aktivierungsserver
  - Vista

Diskussion: Einsatzszenarien
Unternehmen mit 1000 Mitarbeitern

- Naive Berechnung:
  - Windows Server 2008 Enterprise: ~4500 Euro
  - 1000 CALs: ca. 25 Euro/ Stück: ~25.000 Euro
  - Lizenzkosten: 30.000 Euro je ActiveDirectory Server
- Lohnt sich für Unternehmen der Einsatz von “Nachbauten” wie Samba4?
  - Ausfallkosten
  - Administrationsaufwand
  - Support
  - Memberserver, Standort-DC, Fileserver?

Vielen Dank für die Aufmerksamkeit

Sources

- SerNet, Enterprise Samba
  - http://enterprisesamba.com/
- Samba Projekt Wiki
  - http://wiki.samba.org
- Active Directory Übersicht
  - http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx
- Active Directory Betriebshandbuch
  - http://www.microsoft.com/germany/technet/prodtechnol/windowsserver/technologies/featured/ad/active-directory-betriebshandbuch-00.mspx