Fedora/RedHat Directory Server

Ein technischer Überblick von Jens Kühnel

E-Mail: fds kuehnel.org

Jens Kühnel
Konsult und Training
Bad Vilbel Germany

Über den Autor

Jens Kühnel

- Start der Computer-”Kariere” mit 8 Jahren
- Linux Benutzer und -Admin seit 1995
- freiberuflich tätig seit 1999
- zertifizierter RedHat, SuSE/Novell und Microsoft Trainer
- RHCE, RHCA #8, RHCX, SCLT, MCSE, MCT
- Buchautor von:
  Samba 3 – “Wanderer zwischen den Welten“

Aufbau

- Einleitung
- Architektur
- Baum und Bäume
- Zweig und Blatt
- Vergleiche

Einleitung

- **Einleitung**
- Architektur
- Baum und Bäume
- Zweig und Blatt
- Vergleiche

RedHat kauft Netscape-Produkte

- Directory-Server
- Zertifikat-Server
- Mail-Server
- Messaging-Server

- Zur Zeit ist nur der Directory-Server als OpenSource freigeben
- Der Netscape-DS wurde lange Zeit zusammen mit Sun unter den Name iPlanet entwickelt
  - Die Ähnlichkeit zwischen Sun-DS und FDS sind nicht zu verkennen

RedHat oder Fedora Directory Server

- Fedora-Directory-Server (FDS)
  - Wird von der Community entwickelt
  - Kein kommerzieller Support von RedHat
  - Benötigt Java (Sun/IBM)

- RedHat-Directory-Server (RH-DS)
  - Kommerzieller Support von RedHat
  - Minimale Unterschiede zu FDS
  - Ein RPM enthält alles

Doku

- Sehr umfangreiche Doku
  - Handbücher RedHat-Directory-Server mit über 2000 Seiten (auch für FDS benutzbar): http://directory.fedora.redhat.com/
  - Wiki für Fedora-Directory-Server: http://www.redhat.com/docs/manuals/dir-server/

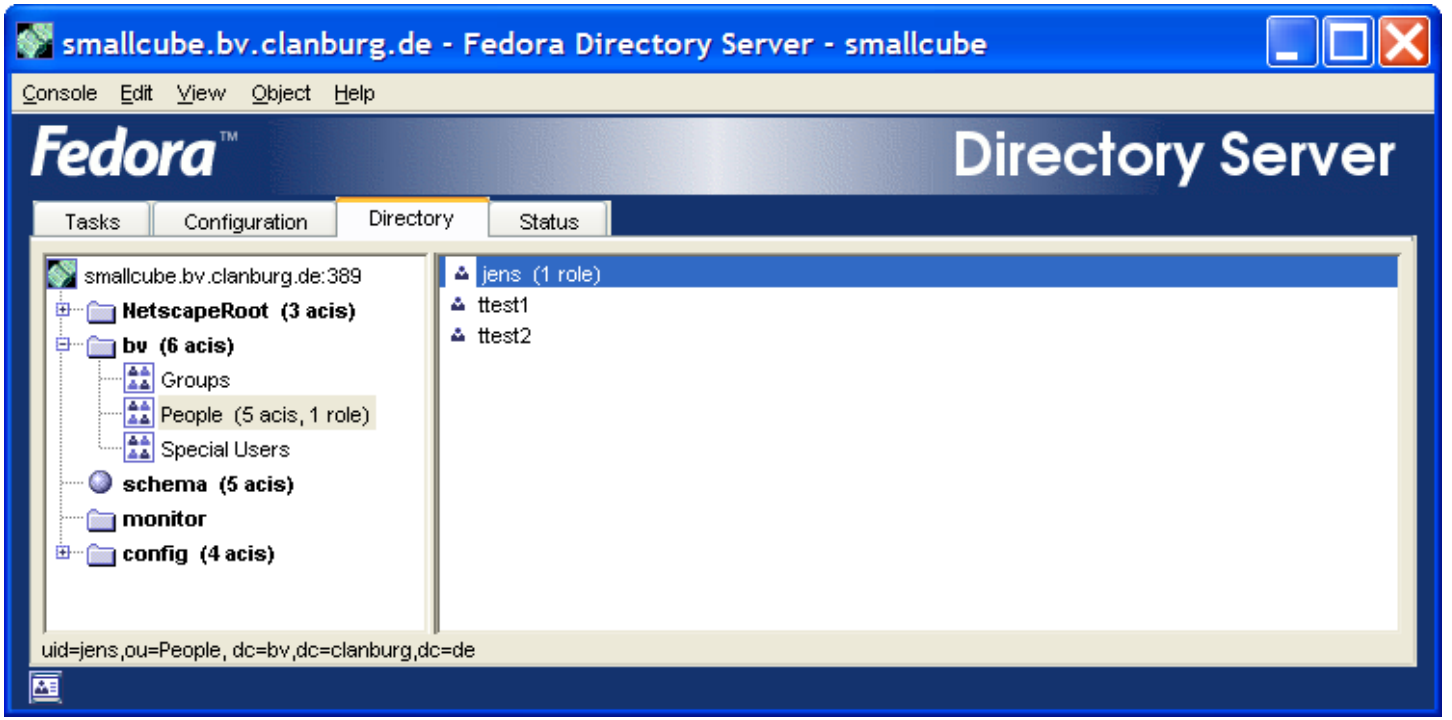
Architektur

- Einleitung
- **Architektur**
- Baum und Bäume
- Zweig und Blatt
- Vergleiche

Architektur Übersicht

- Admin-Console
- Admin-Server
- Directory-Server (NS-SLAPD)
- Berkeley DB mit B-Tree

Admin-Console und -Server



- Admin-Server
  - verwendet httpd.worker
  - Ein Admin-Server für viele Directory-Server

Directory-Server

- Erweiterbar durch Plugins
- SSL inklusive Login mit Zertifikaten möglich
- Backup und Restore online möglich
- hochperformantes Logging

Directory-Server 2

- Sehr große Datenbanken möglich (mehrere GB)
- FDS speichert alle Informationen im LDAP (wichtig bei Replikation)
  - ACIs
  - Konfiguration des LDAP-Baumes
  - Replikations-Konfiguration

Plugins

- Ermöglicht Erweiterungen ohne Änderungen des Server-Core
- Viele Funktionen des FDS sind als Plugin enthalten:
  - Passwordhashes
  - Syntax-Checker u.v.w.
- Interessante weiter Plugins (noch nicht aktiviert)
  - Referential Integrity Plugin
  - Attribute Uniqness Plugin

Bau und Bäume

- Einleitung
- Architektur
- **Baum und Bäume**
- Zweig und Blatt
- Vergleiche

Baum und Bäume

- Multi-Master-Replikation
- Fractial Replikation
- Chaining und Referals
- Virtual Views
- Sync mit ADS

Replikation

- Multi-Master-Replikation
  - jeder Master nimmt Schreibzugriffe entgegen und gleicht sie mit den anderen Mastern ab
  - bis zu 4 Master möglich
  - dadurch sehr hohe Ausfallsicherheit
  - Schreibvorgänge auch bei Ausfall eines oder mehreren Masters weiter möglich

Replikation 2

- Beliebig viele Slaves möglich
- Performance Steigerungen durch viele schreibgeschützte Kopien
- Replizierung kann Zeit gesteuert oder Ununterbrochen erfolgen.
- Einschränkung der Replikation auf Attributsebene möglich
  - Bandbreitenbeschränkung (z.B. keine JPG-Bilder)
  - Sicherheit (z.B. keine Passwörter in die DMZ)

Chaining und Referals

- Referals
  - Informiert den Client, dass gewünschte Informationen auf einem anderen Server liegen
  - LDAP-Standard
- Chaining
  - Fragt im Namen des Clients bei anderem Server nach und gibt Info an Client weiter (quasi ein Proxy)
  - FDS spezifisch

Virtual Views

- Ermöglicht Anpassung an neue Gegebenheiten ohne das echte Änderungen gemacht werden müssen

- Bestehende Objekte können in einem virtuellen Zweig anhand von Attributen neu organisiert werden

Sync mit ADS

- FDS kann mit Microsoft Servern Daten synchronisieren
- Sowohl Windows ADS als auch NT4 werden unterstützt
- Benötigt aktiviertes SSL
- Bei ADS können auch Zweige einzeln synchronisiert werden
- Einige Limitierungen sind bei ADS und NT4 zu beachten

Zweig und Blatt

- Einleitung
- Architektur
- Baum und Bäume
- **Zweig und Blatt**
- Vergleiche

Zweig und Blatt

- Gruppen und Rollen
- Mehrsprachigkeit
- Attribut Encryption
- Password Policy
- Class of Services
- userattr

Gruppen

- Gruppen
  - Definieren der Gruppenmitglieder in der Gruppe
    - UniqueMember = usera, userb
  - Client muss für jedes Mitglied eine eigene Anfrage stellen

Rollen

- Rollen
  - Beim jeweiligen Objekt wir ein Attribut hinzugefügt
  - Z.B. Mitglieder der Rolle *admin*
    - *nsRole: admin*
  - Client kann direkt nach Informationen aller Benutzer mit *nsRole=admin* suchen
  - Verschiedene Formen von Gruppen sind verfügbar
    - Managed
    - Filtered
    - Nested

Mehrsprachigkeit

- Ermöglicht Einträge für das selbe Attribut, in unterschiedlichen Sprachen z.B.

- Full Name;lang-de: Jens Kühnel
- Full Name;lang-en: Jens Kuehnel

Attribut Encryption

- Verschlüsselung einzelner Attribute auf Festplatte möglich
- Schutz vor Diebstahl der Festplatte oder der Backup-Medien
- nur möglich mit aktiviertem SSL
- Verschlüsselung der Attribute erfolgt mit dem Privat-Key des Servers.
- Daher PrivatKey mit PIN/Passwort sichern!

Password Policy

- automatische Sperren/Entsperren von Accounts
- Passwort History
- Auswählbare Passwort „Verschlüsselung“/Hash

Class of Services

- Ermöglicht ein Attribut einmal zu speichern und bei vielen Objekten zu verwenden
- Typischer Fall: Fax-Nummer
- Verschiedene Arten:
  - Sample
  - Indirect
  - Classic

userattr

- Ermöglicht ACIs die auf gespeicherten Attributen des Zieles basieren
- Typischer Fall: Chef
  - Das Objekt *Karl* hat ein Attribut *manager: cn=Peter...*
  - Mit Hilfe des speziellen ACI-Syntax *userattr* ist es möglich dem jeweiligen Manager spezielle Rechte zuzuweisen
  - *Peter* kann Änderungen am Objekt *Karl* durchführen

Vergleiche

- Einleitung
- Architektur
- Baum und Bäume
- Zweig und Blatt
- **Vergleiche**

Vergleiche

- „Probleme“ von FDS
- FDS – OpenLDAP
- FDS – Sun DS
- FDS – ADS
- FDS – Novell eDir

„Probleme“ von FDS

- SSL-Probleme
  - Ist vorgefertigt für den RedHat-Certification-Server
    - Daher keine OpenSSL/GnuTLS Zertifikate direkt möglich
- Benötigt relative viel RAM auch bei kleinen Installationen (256MB)
- Keine /etc/init.d/ Startskripte mitgeliefert
- Die Konfiguration ist in LDAP abgelegt, daher manchmal Probleme bei der Fehlersuche
- Lizenz für Entwickler (Rechteabtretung an RH)

und Open LDAP ??

- Kleiner
- Schneller auf langsamen Maschinen
- Performance Probleme bei großen Installationen (wenn nicht optimiert wurde)
- Standardkonformität geht über alles

Sun-DS

- Durch gemeinsame Entwicklung bei iPlanet sehr viele Gemeinsamkeiten
- Echt Unterschiede zwischen FDS und Sun DS 5.2
  - Sun DS 5.2 hat das Replikationsprotokoll geändert
    - *legacy replication* immer noch mit FDS möglich
  - Internes Datenbank-Format wurde geändert
    - Komplett Backup von Sun-DS und Restore mit FDS funktioniert

eDir und ADS

- Beide Directories haben umfangreich Zusatzfunktionen
- Stark integriert in die entsprechenden Umgebungen:
  - ZEN usw.
  - Exchange, MS-SQL usw.
- Beide verwenden Multimaster-Replikationen mit beliebig vielen Mastern (async)

Novell eDir

- Grundlage für eigenen Authentifizierungsdienst
- LDAP aufgesetzt
  - Verwendet schon Verzeichnisse länger als es LDAP gibt
- Umfangreichere Replikationskontrollen
- Closed Source
- Preis

Microsoft ADS

- ADS = LDAP + Kerberos + ActiveSync
- LDAP mit sehr umfangreichen und seltsamen Schema
- Synchronisierung mit FDS möglich
- Closed Source
- Preis