FUDConBrussels

Fedora/ RedHat Directory Server

by Jens Kühnel (Germany)

About Jens Kühnel

- Stating the computer “carrier” with 8
- Linuxuser and Linuxadmin since 1995
- Freelancing Trainer since 1999
- Certified RedHat, SuSE and Microsoft Trainer
- RHCE, RHCA#8, RHCX, SCLT, NCLE10, MCSE, MCT
- Author of a German Samba3 book

Index

- **Introduction**
- Architecture
- Tree
- Branch and Leave
- Compare

RedHat buys Netscape products

- Directory server
- Certificate server
- Mail server
- Messaging server

- Only Directory server is GPL´ed at the moment
- Netscape DS was developed together with sun for some time aka iPlanet.
  - Sun-DS and FDS are quite similar

Fedora vs. RedHat

- Fedora Directory Server (FDS)
  - Improved by the community
  - No commercial support from RedHat
  - Needs external Java (Sun/IBM)
- RedHat Directory Server (RH-DS)
  - Commercial supported by RedHat
  - The RPM includes everything (incl. Java)

Documentation

- Very extensive Documentation
  - RedHat directory server handbook are 2000 Pages strong
    Usable for FDS as well
    http://www.redhat.com/docs/manuals/dir-server/
  - Wiki for Fedora-Directory-Server
    http://directory.fedora.redhat.com/

Architecture

- Introduction
- **Architecture**
- Tree
- Branch and Leave
- Compare

Architecture Overview

- Admin-Console
- Admin-Server
- Directory-Server (NS-SLAPD)
- Berkley DB with B-Tree

Admin-Console and -Server

- Admin-Server
  - Uses httpd.worker
  - One Admin Server for every machine

Directory-Server

- Extensible with PlugIns
- SSL inclusive Login with Certificate possible
- Backup and restore online
- Syslog-free logging

Directory-Server 2

- Very big Databases possible (multi Gbs)
- FDS stores everything in LDAP
  - ACIs
  - Configuration for LDAP trees
  - Replication configuration

Plugins

- Possibility to improve Server without changing the core
- A lot of functions are really plugins:
  - Password hashes
  - Syntax Checkers etc.
- Other interesting plugins (needs activation)
  - Referential Integrity plugin
  - Attribute Uniqness plugin

Tree

- Introduction
- Architecture
- **Tree**
- Branch and Leave
- Compare

Replication

- Multi-Master-Replication
  - Every master can write and syncs with other masters
  - Up to 4 masters are possible
  - High availability
    - even when a master is down writes are possible

Replication 2

- As many slaves as you like
- Replication can be time controlled or uninterrupted
- Replication can be limited at attribute level:
  - Bandwidth limitation (like JPEG-Pictures)
  - Security (no password in DMZ)

Chaining and Referrals

- Referrals
  - Informs the requesting client where the inforation can be found
  - LDAP standard
- Chaining
  - Asks an other server in the name of the client and gives the information to the client
  - FDS specific

Virtual Views

- Makes it possible to change the Tree without changing it
- Existing objects can be rearrange in a virtual tree

Sync with ADS

- FDS can synchronize User/Groups with Microsoft Servers
- Supports Windows DAS and NT4
- Needs SSL and a small Program at the MS Server
- Single trees can synchronized
- Some limitations applies at ADS and NT4

Branch and Leave

- Introduction
- Architecture
- Tree
- **Branch and Leave**
- Compare

Group

- Defining the group membership inside the group
  - UniqueMember = usera
  - UniqueMember = userb
- Client has to search for every member attribute individual

Roles

- Every object gets extended with a special attribute
- For example: nsRole:admin
- Client can search for every user with nsRole=admin
- Different “kinds” are available
  - Managed, Filtered, Nested

Multi language

- Multiple Entries for the same Attribute is possible for different languages:
-
- Full Name; lang-de: Jens Kühnel
- Full Name; lang-en: Jens Kuehnel

Attribute encryption

- Encryption of single attribute at the hard disc
- Secures against theft of hard disc and of backup-media
- Only possible with activated SSL
- Uses the server private key for encryption
- Please secure private key with PIN/Password

Password policy

- Automatic locking/unlocking of accounts
- Password history
- Selectable password hashes

Class of Services

- Makes it possible to save an attribute only once and uses it at a lot of objects
- For example: fax number
- Different kind:
  - Simple
  - Indirect
  - Classic

Userattr

- Creates ACI´s based on the attributes of the target
- Typical case: the boss
  - Object/user Carl has an object like manager: cn=Peter, ...
  - Userattr make it possible to allow Peter to change all object he is manager of

Compare

- Introduction
- Architecture
- Tree
- Branch and Leave
- **Compare**

“Problems” with FDS

- SSL-”Problem”
  - Is prepared for RedHat Certification Server
    - OpenSSL/GnuTLS have to be converted to PKCS#12
- Needs a lot of ram (256MB/1024MB)
- No /etc/init.d/ start script shipped
- Configuration is saved in LDAP, problem at troubleshooting
- License (Contributor License agreement)

And OpenLDAP?

- Smaller memory footprint
- Faster on slow machines
- Performance problems when not tuned
- Standard conformity above all

Sun-DS

- Shared ancestor IPlanet
- Real different between FDS and SUN DS5 is
  - Sun DS 5.2 uses different replication protocol
    - Legacy replication still works
  - Internal DB Format has changed
    - Complete backup and restore works

eDir and ADS

- Both Directory's have extensive addons
- Highly integrated in there environment
  - ZEN etc.
  - Exchange, MS-SQL etc.
- Both are using Multi master replication with a lot of masters (async)

Novell eDir

- Basis for the own authentication server
- LDAP is an add on
  - They directory's exist longer then LDAP
- Extensive replication control
- Closed Source
- Price

Microsoft ADS

- ADS = LDAP + Kerberos + ActiveSync
- LDAP with very extensive and “strange” schema
- synchronization with FDS is possible
- Closed Source
- price


The fedora™ team