Is the Apache Directory Server the new challenger to FedoraDS and OpenLDAP?

Emmanuel Lécharny
Iktek
<elecharny@iktek.com>
Planning

• 1- Introduction
• 2- Features comparison
• 3- Compared performances
• 4- Future evolutions
• 5- Conclusion...
• 6- Q&A
1-Introduction
2-1 Functionalities
Generalities

<table>
<thead>
<tr>
<th>LdapV3</th>
<th>Code</th>
<th>Documentation</th>
<th>Books</th>
<th>Licence</th>
<th>Backed by organization</th>
<th>Origin</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ApacheDS</td>
<td>FedoraDS</td>
<td>OpenLDAP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>checked</td>
<td>checked</td>
<td>checked</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Java</td>
<td>C/C++</td>
<td>C/C++</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Well, err...</td>
<td>Extensive</td>
<td>Spare</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>None</td>
<td>None</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ASL 2.0</td>
<td>GPL</td>
<td>OPL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Apache</td>
<td>RedHat</td>
<td>Many</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Genuine</td>
<td>Michigan university</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Technical elements

<table>
<thead>
<tr>
<th>Feature</th>
<th>ApacheDS</th>
<th>FedoraDS</th>
<th>OpenLDAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation</td>
<td>Installer</td>
<td>Installer</td>
<td>Package/build</td>
</tr>
<tr>
<td>Backend JDBM</td>
<td>✗</td>
<td>RDBMS allowed</td>
<td>BDB, GDB...</td>
</tr>
<tr>
<td>Transaction RDBMS</td>
<td>✗</td>
<td>RDBMS</td>
<td>Extension</td>
</tr>
<tr>
<td>Multi-backend</td>
<td>✗</td>
<td>Yes</td>
<td>✗</td>
</tr>
<tr>
<td>Replication Mitosis M/M</td>
<td></td>
<td>4 ways M-M</td>
<td>M-S</td>
</tr>
<tr>
<td>Schema Compilation Dynamic/GUI</td>
<td></td>
<td></td>
<td>Static/files</td>
</tr>
<tr>
<td>Referrals</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Attribute Encryption</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Subtrees specification</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
</tr>
</tbody>
</table>
## Security

<table>
<thead>
<tr>
<th>Feature</th>
<th>ApacheDS</th>
<th>FedoraDS</th>
<th>OpenLDAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL V3</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>TLS</td>
<td>Soon...</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>SASL</td>
<td>Soon...</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>ACIs</td>
<td>✔️</td>
<td>✔️</td>
<td>Partial?</td>
</tr>
<tr>
<td>Attribute Encryption</td>
<td>❌</td>
<td>✔️</td>
<td>❌</td>
</tr>
</tbody>
</table>
2-2 Apache DS
Apache DS structure
Apache Directory Server

- Full RFCs compliance
- Embeddable
- Layered architecture
- Extensible (Kerberos, DNS, DHCP...)
- Implements X500 Administrative model
- Written in Java => multi-platform
Apache DS X500 extensions

• X.500 Directory Administrative Model
• Basic Access Control Scheme
• Collective Attributes
• Subentries
Subentries

- Selections
- Exclusions
- Levels
- Filtering
- ...
ADS drawbacks

- It's young!
- Lot of bugs to be fixed (memory leaks)
- Replication is to be delivered by October
- Large object remains in memory
- Backend: JDBM only at the moment
- Documentation is lacking
- It's a large piece of software, and we are few working on it...
3- Performance
Tests

- 3 tests:
  - Added 10K users
  - Random search through the base
  - Delete all the 10K users
  - “Out of the box” installation
  - We just wanted to know if we are really bad ;)
Users

- Use of MakeLdif to create users:

dn: uid=user.3776,ou=People,dc=cs,dc=hacettepe,dc=edu,dc=tr
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
givenName: Janeczka
sn: Favreau
cn: Janeczka Favreau
initials: JF
uid: user.3776
mail: user.3776@cs.hacettepe.edu.tr
userPassword: password
telephoneNumber: 510-586-6567
homePhone: 143-449-3159
pager: 012-704-9314
mobile: 105-287-9092
employeeNumber: 3776
street: 55438 Ash Street
l: Steubenville
st: MT
postalCode: 77097
postalAddress: Janeczka Favreau$55438 Ash Street$Steubenville, MT 77097
description: This is the description for Janeczka Favreau.
Typical search request

• Search for a single user, randomly picked
• Perform 10K searches
  • The cache is not likely to be used at run 1
• 10 runs
• The fastest and slowest are removed

uid=user.@,ou=People,dc=cs,dc=hacettepe,dc=edu,dc=tr
Insertion/deletion

Add 10K users

Delete 10K users

(Smaller pyramids is better)
Search run

Ldap servers performance test: random search
Performance issues

- Better cache mechanism needed
- ASN.1 codec can be improved (15% total)
- Needeless Attribute checking (12% total)
- DN processing optimization (10% total)
- Serialization improvement
- Some operations are done many times
- Backend is not optimal
- Memory allocation => GC
What has already been done

- DN comparison improved: ADS 4x times faster !!! (with a single line modified :)
  - One day to work this out
  - Thanks to yourKit profiler!
- ASN.1 codec is much faster (10x)
  - 6 months of work, 40 000 SLOCs
- LdapDN is 2.7x faster than LdapName
  - 2 months of work, difficult to merge in ADS :(
4- Evolution
Backend

• JDBM is the actual backend
• Berkely DB JE© is a possible target
• RDBMS soon...
• Needs:
  • Fast backend
  • Reliable backend
  • Transactions support
Tooling (RCP- Eclipse plugin)

- Start/Stop
- Import/export
  - LDIF
  - DSML 1.0/2.0
- UI Schema Manager
- Ldap Browser
- Ldap Proxy
Replication

• Replication is a must-have
  • Master-Slave replication (OpenLDAP) OR
  • Multi-Master replication (FDS)

• RFC 3384 => Multi Master replication
• Draft by Zeilenga says : 'LDAP Multi-master Replication Considered Harmful'

• What about ADS ?
SP and Triggers

• SP : stored procedure
  • Support Java language, but scripting languages as Janino or Jython may be added later
  • Ease some management operations
• Triggers with pre/post operations
  • Fine grained replication
  • E-Provisioning
Standards

• New RFCs: RFCs 4510 -> 4519
  • Better X500 compliance
  • Internationalization explained
  • Clarification on previous RFCs
  • Imply some modification, but not so much.

• Collectives attributes support (RFC 3671)

• Subentries support (RFC 3672)
5-Conclusion
Links

• Apache Directory Server site and documentation:
  • http://directory.apache.org/
  • http://directory.apache.org/subprojects/apacheds/features.html
  • http://directory.apache.org/subprojects/apacheds/index.html
  • http://directory.apache.org/subprojects/mina/index.html

• Articles
  • http://www-128.ibm.com/developerworks/opensource/edu/os-dw-os-ag-ld;
  • http://www-128.ibm.com/developerworks/java/library/j-apacheds1/
  • http://www-128.ibm.com/developerworks/java/library/j-apacheds2/
Thanks!

- **Alex Karasulu**, “the brain”!
- **Trustin Lee**, Mina's father
- **Ersin Er**, Sp and Triggers
- **Stefan Zoerner**, tests and docos
- **Brett Porter**, Maven and now MVN :)
- And **Peter Royal**, **Cyrille Leclerc**, **Stéphane Bailliez**, **Pierre-Arnaud Marcelot** for their help and support!

Special thanks to **Zinedine Zidane**!