Identity Services with OpenDS

Ludovic Poitou

Software Architect
Sun Microsystems, Inc.
http://www.opends.org

Goal of Your Talk

What Your Audience Will Gain

Learn about the OpenDS project and discover some unconventional use of an LDAP directory server.

Agenda

Introduction to OpenDS

Cool Stuff built with OpenDS

Agenda

Introduction to OpenDS

Cool stuff built with OpenDS

What is OpenDS ?

- It's an Open Source project
  - initiated by Sun
  - to build a 100% pure Java, highly scalable, providing high performance, easy to use LDAPv3 based Directory Service
  - released in open source under the CDDL license in July 2006
- OpenDS is the foundation of the next generation of Sun Directory Services

OpenDS today

- Version 0.8 released
  - Fully functional LDAPv3 server
  - Already supports many extensions
  - Access Controls compatible with Sun Directory Server
  - Multi Master Replication
  - Installs in a few seconds
- The Community
  - 22 commiters, 12 external contributors
  - 145 registered users

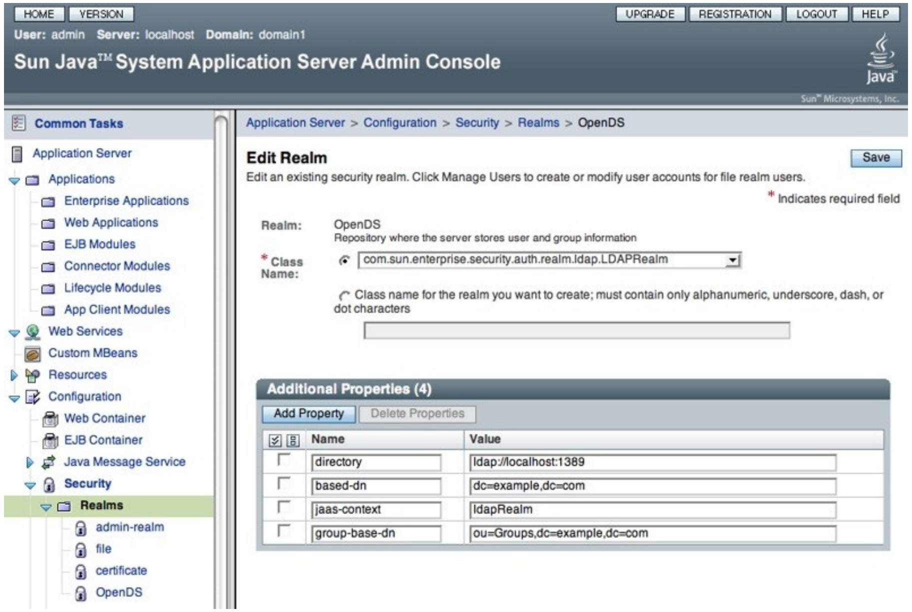
Agenda

Introduction to OpenDS

Cool stuff built with OpenDS

Glassfish and OpenDS

- Used to authenticate and authorize users
- Leverage the LDAPRealm in Glassfish



Edit Realm

Edit an existing security realm. Click Manage Users to create or modify user accounts for file realm users.

* Indicates required field

Realm: OpenDS
Repository where the server stores user and group information

* Class Name: ● com.sun.enterprise.security.auth.realm.ldap.LDAPRealm

○ Class name for the realm you want to create; must contain only alphanumeric, underscore, dash, or dot characters

Additional Properties (4)

☑	Name	Value
□	directory	ldap://localhost:1389
□	based-dn	dc=example,dc=com
□	jaas-context	ldapRealm
□	group-base-dn	ou=Groups,dc=example,dc=com

- See http://blogs.sun.com/treydrake/entry/glassfish_opends_integration

OpenID Identity Provider

- LDAP Directories are perfect fit for storing all information of an Identity Provider.
- A servlet implements an OpenID Identity Provider service
  - Initially implemented from scratch,now uses OpenID Extension for OpenSSO (contributed by Paul Bryan)
- Leverages OpenDS for creating, searching users, authenticating them and storing sessions over LDAP (using Mozilla LDAP Java SDK)

Atom Server

- A Servlet implements Atom Publishing Protocol and leverages OpenDS for the storage and retrieval of atom entries
- REST interface : RFC 4514 LDAP URL
- So the query is an LDAP URL and the server returns an Atom with the entries:
  - List all users from a Directory
  - List all entries that have changed in the last 5 minutes
- Built with ROME 0.9 and Mozilla LDAP Java SDK

Summary

- OpenDS provides a hierarchical database with high availability built in and a standard access protocol
- It is at the core of Identity Services such as OpenSSO and OpenID
- But it could be used in many other innovative ways

For More Information

- Open Identity booth today and during JavaOne
- http://www.opends.org
- Blogs:
  - http://blogs.sun.com/treydrake
  - http://blogs.sun.com/DirectoryManager
  - http://blogs.sun.com/Ludo