OpenDS Introduction

David Ely
Directory Services
Sun Microsystems, Inc.

What is OpenDS?

- Open source community project building a free and comprehensive next generation directory service
- Designed to address large deployments, to provide high performance, to be highly extensible, and to be easy to deploy, manage, and monitor
- A directory service that will include all the essential directory-related services like directory proxy, virtual directory, data distribution, and data synchronization
- Eventually, Sun's next generation directory service

What to get out of this presentation

- A basic understanding of LDAP
- How LDAP compares to RDBMS
- An LDAP server is the best repository for many applications
- Sun has long been the market leader in LDAP servers
- OpenDS is continuing that trend

LDAP Essentials

- Historically, each application had its own database with user data
- An LDAP directory service centralizes this user data
  - Accessible over a standard protocol
  - Common data is shared, while applications can extend what's stored (e.g. inetOrgPerson + posixUser for Unix account data).

LDAP Essentials

- LDAP presents data as a Hierarchical Database
  - Unit of storage is an **Entry** which is a collection of **Attribute** values
  - Directory Information Tree (**DIT**) defines how the hierarchy is structured (e.g. flat or nested)
  - Every entry has a single parent and a naming attribute, whose value is unique among siblings
    - Relative Distinguished Name (**RDN**)
  - Entry's RDN and those of its ancestors uniquely identify it
    - Distinguished Name (**DN**)
    - uid=jgosling,ou=smart people,ou=people,dc=sun,dc=com

LDAP Essentials

- Lots of advanced features
  - virtual attributes, extensibility, strong authentication
- Originally, optimized for reads and searches
- Write performance is catching up and customers want more
  - E.g. Telcos updating your LDAP entry every time you move between cell towers

LDAP Directory & RDBMS Similarities

- Persistent, reliable, remotely-accessible, performant store for arbitrary data

RDBMS	LDAP
Insert	Add
Query	Search
Row	Entry
Column	Attribute
Table	*Objectclass*
WHERE lastname='Green' AND firstname='Rich'	(&(sn=Green) (givenname=Rich))

RDBMS Features not in LDAP

- Transactions can span updates to multiple rows/tables
  - LDAP: updates to one entry are atomic, Internet Draft for LDAP Transactions
- More powerful queries
  - Joins across tables
- Better with arbitrary data

Additional LDAP Features

- LDAP is a wire-protocol
  - Client doesn't depend on server
- More flexible schema
  - Entries/attributes are not fixed-sized
  - Multi-valued attributes
  - On-the-fly schema changes
- Identity focused
  - Standard user-centric schema
  - Authentication, authorization, and auditing
  - Password policy
  - Groups and Role-Based Access Control

History of Directories at Sun

- x500 Directory (1988)
  - > Standard from International Telecommunication Union
  - > Complex, few full implementations (Sun Solstice 1996)
- Lightweight Directory Access Protocol (LDAP)

  - > Similar to x500, but simpler
  - > University of Michigan 1991
- Netscape Hires all U-Mich Employees 1996

  - > NS DS 1.0 in 09/1996, 3.0 in 02/1998, 4.0 in 10/1998
- Sun takes on LDAP (based on U-Mich):

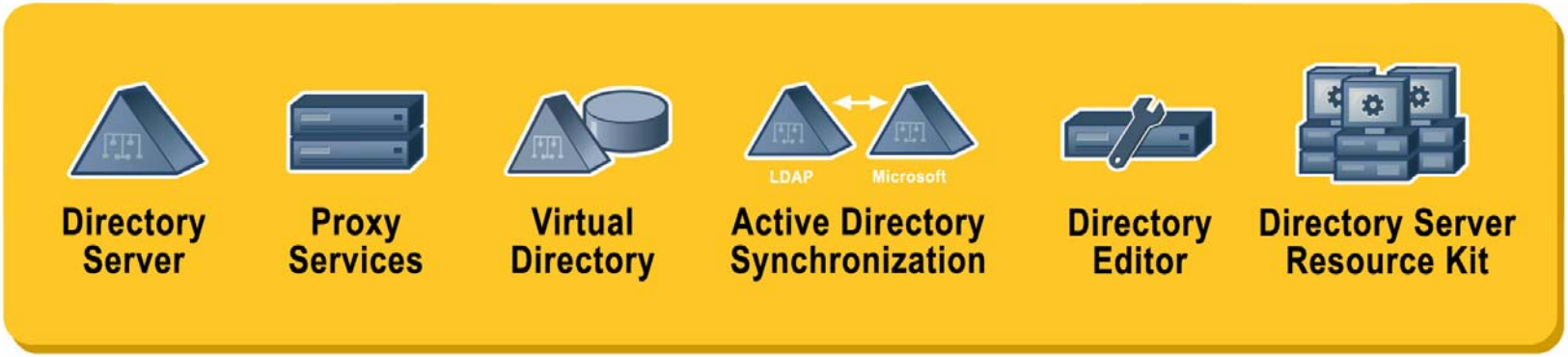
  - > Sun Directory Services 1.0 ships in 09/1997
  - > Sun Directory Services 3.1 ships in 07/1998

History of LDAP at Sun

- Sun | Netscape Alliance (1999-2002)
  - iPlanet Directory Server 5.0/5.1 based on Netscape Code
- Sun ONE Directory Server 5.2 (2003)
  - 5.2 patch 2 (2004)
  - 5.2 patch 3 & 4 (2005)
- Sun Java System Directory Server 6.0 (2007)

DSEE 6

- Suite of market-leading, mature, stable, high-performance, standards-compliant, easy-to-manage, highly-available, secure directory products
- 2500+ customers
  - > Used by majority of top Financials, Telcos, Auto-makers, Airlines, Pharmaceuticals



OpenDS Goals

- OpenDS should ***"Exceed DSEE 6 in every way"***

- Competitive Goals
  - Multi-generation leap over competition
  - Un-matched performance and scalability
  - Developer-centric & Deployer-friendly
  - Detailed Instrumentation
- Design Goals
  - Development/release agility
  - 100% pure Java
    - Platform Independence
    - Fit for personal, telco, and embedded deployments
  - Build open source community before initial release

OpenDS Project Details

- OpenDS is hosted at java.net where it's the 4th most active project
- Community
  - 135 registered users – download and use OpenDS
  - 24 committers – direct access to the repository
  - 8 external contributors – provide content w/o direct access
- Issue Tracker, Java 1.5, Ant, Subversion,TestNG, EMMA
- Released under CDDL license

OpenDS Timeline / Roadmap

- 1/2005: OpenDS started
  - Very small “skunk works” project
- 7/2006: OpenDS released as open source
- 9/2007: OpenDS 1.0 beta
- 12/2007: OpenDS 1.0 release

OpenDS Now

- LDAP v3 compliant directory
- Multi-master replication
- Access Controls
  - configurable over protocol
  - proven model used by Sun DS and Fedora
- Support for numerous RFCs and standard controls
- Extensive automated test suite
  - Unit, functional, and system tests

OpenDS Supported Standards

RFC 1274 RFC 1321 RFC 2079 RFC 2222 RFC 2246 RFC 2247 RFC 2251 RFC 2252 RFC 2253 RFC 2254 RFC 2255 RFC 2256 RFC 2307 RFC 2696 RFC 2713 RFC 2714 RFC 2739 RFC 2798 RFC 2829 RFC 2830 RFC 2849 RFC 3045 RFC 3062 RFC 3112 RFC 3377 RFC 3546 RFC 3673 RFC 3674 RFC 3771 RFC 3829 RFC 3876 RFC 3909 RFC 4346 RFC 4370 RFC 4403 RFC 4422 RFC 4505 RFC 4510 RFC 4511 RFC 4512 RFC 4513 RFC 4514 RFC 4515 RFC 4516 RFC 4517 RFC 3698 RFC 4519 RFC 4525 RFC 4526 RFC 4527 RFC 4528 RFC 4529 RFC 4530 RFC 4532 RFC 4616 draft-armijo-ldap-treedelete draft-howard-namedobject draft-howard-rfc2307bis draft-ietf-ldapext-psearch draft-ietf-ldup-subentry draft-ietf-sasl-crammd5 draft-sermersheim-ldap-subordinate-scope draft-wahl-ldap-adminaddr draft-weltman-ldapv3-proxy

Performance Test Setup

- Server Machine
  - V40z: 4 dual-core Opteron 940 CPUs, 32 GB RAM
  - Single internal disk with UFS filesystem
  - Solaris 10 Update 3 (11/06)
  - Java version 1.6.0 build 105 (32-bit)
- Initialization
  - 100,000 entries created using a standard template
- Tests using SLAMD
  - Search: find the single entry that matches a randomly-generated filter
  - Modify: update a single unindexed attribute in a randomly-chosen entry

Performance Results

- Search
  - 20600 – 29700 per second depending on configuration
- Modify
  - 6200 – 6700 per second depending on configuration
- OpenDS was designed and implemented from the ground up to be high performance
- But still room for improvement
  - No performance tuning lately

OpenDS 1.0

- Goal: be the best open source LDAP directory
- Targeted at Enterprise markets, focusing on
  - stability
  - ease of use
  - performance
- Key Features
  - Fully LDAP v3 compliant
  - Multi-master replication
  - Non-GUI administrative interfaces
    - Online configuration changes
- Stable pluggable interfaces

OpenDS Next

- Goal: be the best LDAP directory
- Virtual, Proxy, and Distribution functionality
- GUI for all aspects of management
- More Replication Options (fractional, subtree)
- and much, much more

OpenDS in Interesting Places

- Penrose Virtual Directory is using OpenDS as a front end
  - http://docs.safehaus.org/display/PENROSE10/OpenDS
- JBoss is embedding OpenDS for testing
  - http://jira.jboss.com/jira/browse/SECURITY-5
- Roller and Glassfish can use OpenDS to authenticate
  - http://rollerweblogger.org/roller/entry/configuring_roller_with_opends
  - http://blogs.sun.com/treydrake/entry/glassfish_opends_integration
- Atom (APP) and OpenID gateways
- Maximus Inc. will add OpenDS 1.0 to their portfolio

Questions?

david.ely@sun.com