



# LDAP Proxying and Virtualization – Requirements vs. Capabilities

*GUUG 1<sup>st</sup> Int. Conference on LDAP*  
Cologne, 07-SEP-2007

Andre Posner, Sun Microsystems GmbH  
Robert Polster, Sun Microsystems GmbH



# Agenda

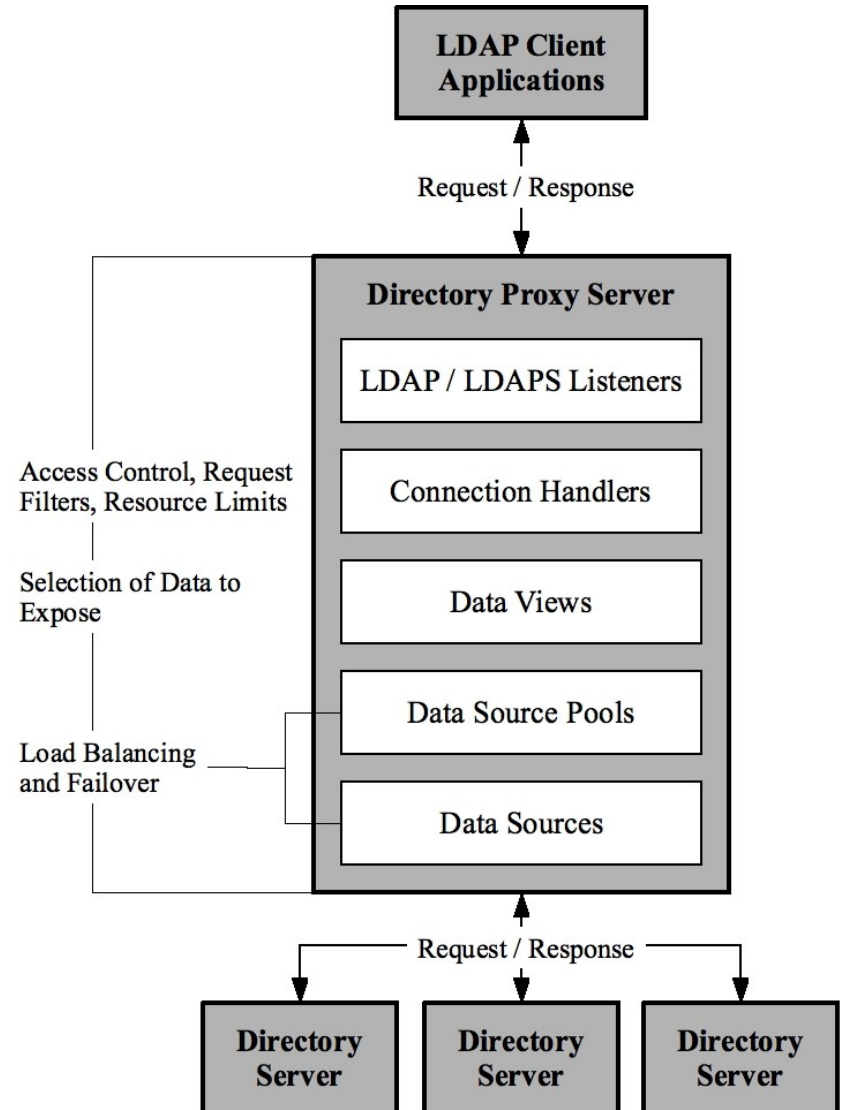
- Terminology
  - > LDAP Proxying
  - > LDAP Virtualization / Virtual Directory
- LDAP Proxying & Virtualization Scenarios
  - > Mitigation of Client Shortcomings
  - > Request Routing and Security
  - > Transparency During Upgrade / Migration
  - > Consolidation of Distributed and Disparate Data Repositories
- LDAP Proxy Deployment
  - > High-Available and Secured LDAP Proxy Topology
  - > Increased WRITE Performance
  - > Reduced Client WAN Access
- Conclusion

# Terminology:

## *LDAP Proxying*

# LDAP Proxying – Characteristics

- Proxy acts as directory service requestor on behalf of its client(s)
- Proxy may alter client request and service response
- Additional features
  - > Traffic Load Balancing
  - > Service Health-Checking
  - > Traffic rerouting and replaying BINDs in case of outages
  - > Access control mechanisms
  - > Data aggregation and abstraction

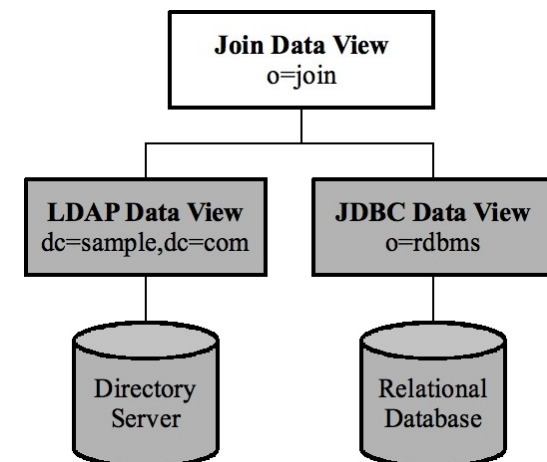
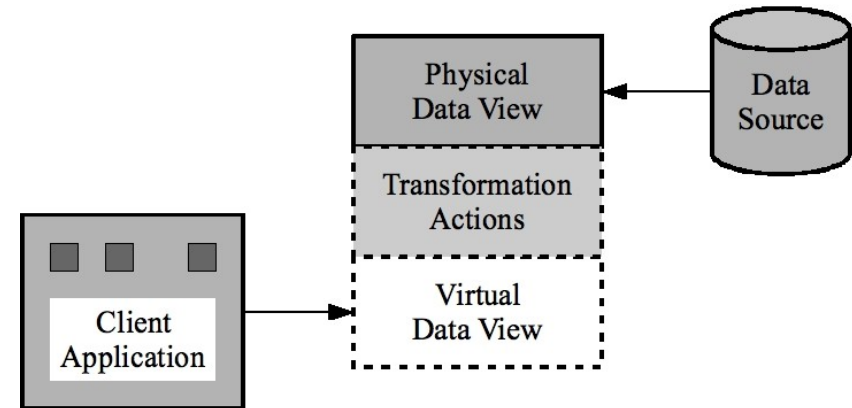


## Terminology:

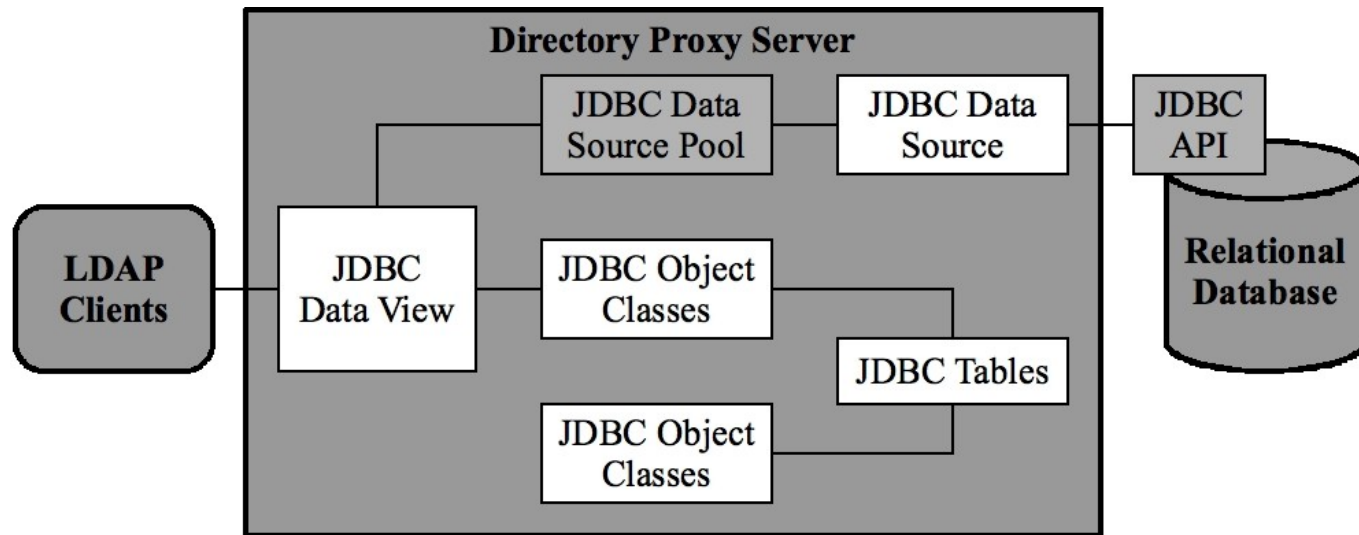
*LDAP Virtualization /  
Virtual Directory*

# LDAP Virtualization – Characteristics

- Core concept: Data Views
  - > Physical Data View
  - > Virtual Data View
    - > Transformation Actions
    - > Properties
  - > LDAP Data Views
  - > LDIF Data Views
  - > Join Data Views
  - > JDBC Data Views (see next slide)
- Virtual Access Control
  - > Connection Classes
- Virtual Schema Checking
  - > Schema Compatibility



# LDAP Virtualization – JDBC Data View



- **JDBC Tables**
  - > represent relational database tables
- **JDBC Object Class**
  - > maps one or more JDBC Tables to an LDAP objectclass
- **JDBC Data View**
  - > aggregates JDBC Object Classes into a single data view

# LDAP Proxying & Virtualization Scenario #1:

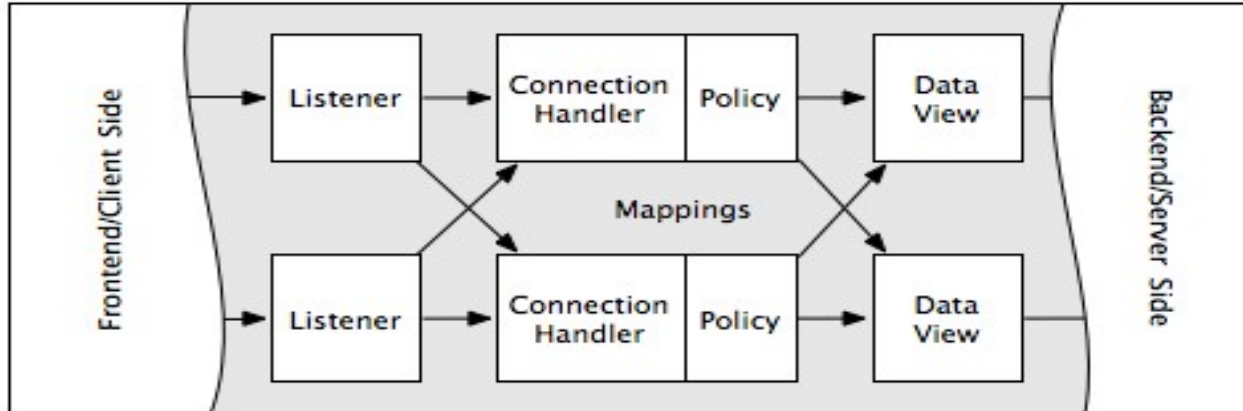
## Mitigation of Client Shortcomings

# Mitigation of Client Shortcomings

- Scenario: *Inabilities of LDAP client applications*
  - > poor LDAP client code quality (design, concept)
  - > clients cannot handle referrals
  - > clients cannot share/reuse established LDAP connections
  - > clients cannot reliably detect service failures (no timely fail-over)
- Remedy: *A modern LDAP proxy*
  - > Automatic/transparent following of referrals
  - > Reliable and configurable health-checking mechanisms
  - > Automatic fail-over/-back to/from directory service instances
  - > Connection Pooling to backend systems
  - > Nice to have: (Partial) BER-decoding of client-originating LDAP requests for increased performance and scalability

# LDAP Proxying & Virtualization Scenario #2: Request Routing and Security

# Request Routing and Security



- Scenario: Hardware load balancer capabilities fall short
  - > Distributed user-base on backends
  - > Optimized directory server tuning for READ, WRITE operations
  - > Different (LDAP) backends implement different access control mechanism
- Remedy: Advanced LDAP loadbalancing features
  - > Combined data view across mutiple backends
  - > Operation type based load-balancing
  - > Homogeneous, fine grained access control established by directory proxy

**LDAP Proxying &  
Virtualization Scenario #3:  
Transparency  
During Upgrade/Migration**

# Transparency During Upgrade / Migration

- Scenario: Impossibility of simultaneous migration of client and server
  - > Missing client required attributes in LDAP backends
  - > DIT redesign required
  - > Different syntax between client and server for the same semantics
- Remedy: Introducing an abstraction layer between client and server
  - > Constructing attributes/-values on-the-fly
  - > Transformation of base-DNs and search filters components in client requests
  - > Transformation of object DNs in server responses
  - > Transformation/Construction of attribute-values in server responses

# LDAP Proxying & Virtualization Scenario #4:

Consolidation of  
Distributed and Disparate  
Data Repositories

# Consolidation of Distributed and Disparate Data Repositories

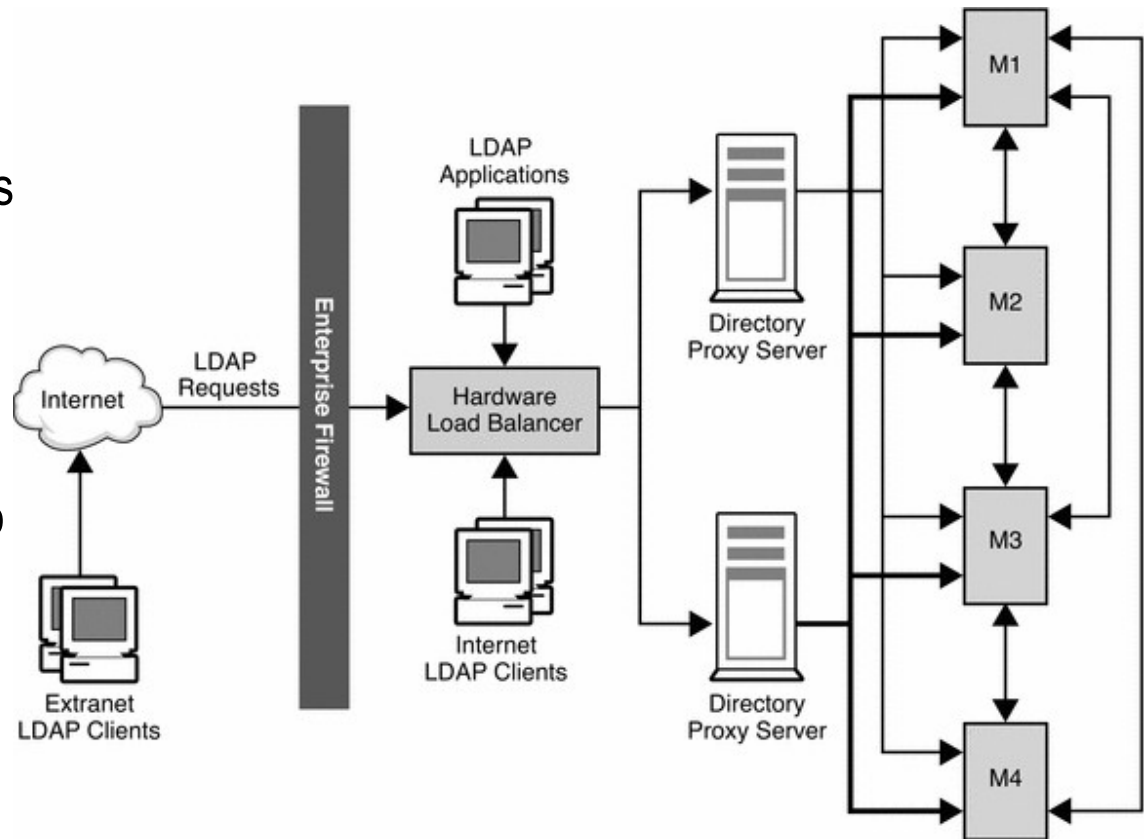
- Scenario: A Company Merger
  - > Demand for an instant and unified view of any merger-relevant data
  - > Lay of the land
    - > Standalone suffixes
    - > dispersed subtrees
    - > data portioned out by distribution logic
    - > disparate data storage technologies (directories, RDBMS, flat files)
    - > schematic discrepancies
- Remedy: *A Virtual Directory*
  - > Virtual Data Views per client application
  - > Join Data Views that aggregate and transform other data views (LDAP, JDBC)
  - > JDBC Data Views that construct and expose a volatile DIT

# LDAP Proxy Deployment

# LDAP Proxy Deployment

## High-Available and Secured LDAP Proxy Topology

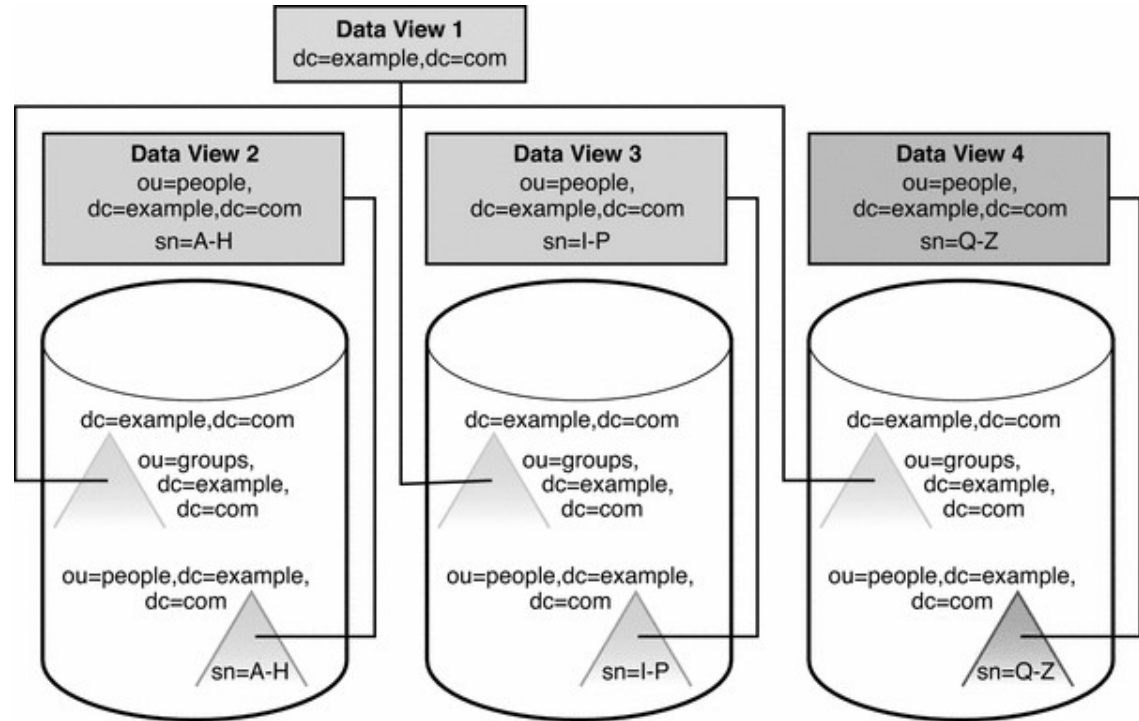
- No *real* data on proxies; can easily be scaled horizontally
- Firewall building block controls extranet access
- Backend directory server accept connections from proxies only
- Client requests are directed to proxy server farm via LB building block; HA on IP level
- Multiple proxy instances to avoid SPoF
- Fully-meshed MM-topology ensures HA on directory server level



# LDAP Proxy Deployment

## Increased WRITE Performance

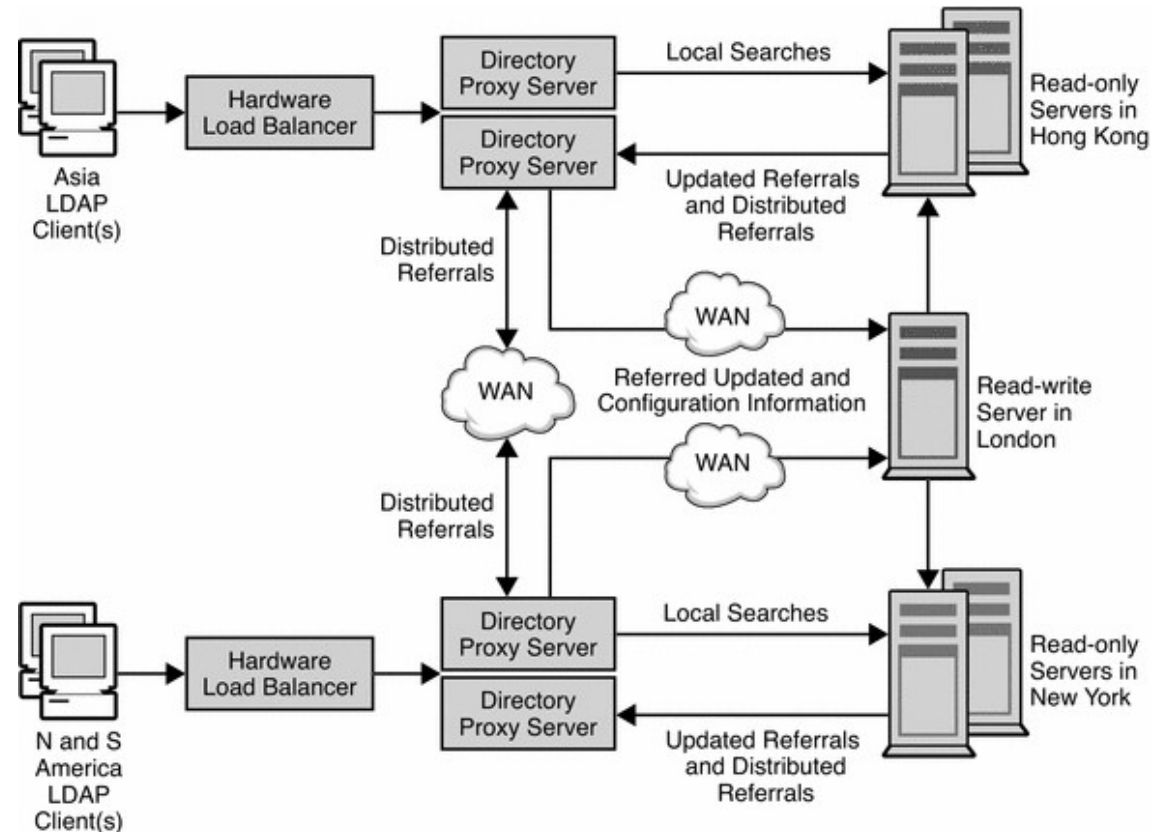
- Directory proxies enable data distribution amongst involved directory server instances
- Distributed data is aggregated on the proxy layer
- Data distribution is a decisive approach to increase WRITE performance on the directory server layer



# LDAP Proxy Deployment

## Reduced Client WAN Access

- Client requests are processed locally, thus reducing network overhead
- Local directory server instances effectively partition directory infrastructure, thus increasing performance and scalability
- Due to automatic following of referrals by proxies, all data appears to be local from a client perspective



# Conclusion

# Sun Directory Proxy Server 6

## We can do it!

- Virtual Directory Capabilities
  - Virtual Directory provides a consolidated virtual view of a users identity across multiple disparate data sources
  - Support for both LDAP directories and databases
  - Ability to read and write data
  - Support for mapping resources into a virtual DIT
  - Enhanced access controls for security and availability
  - Operation routing and load-balancing

**Q & A**

**Your questions, please.**



Thank you.

Andre.Posner@Sun.COM  
Robert.Polster@Sun.COM

