



**Benefits of an Exclusively
Multimaster Deployment of
Sun Java™ System Directory Server
Enterprise Edition 6**

Michael Melore

June 2008

Sun Microsystems, Inc.

Copyright © 2008 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

U.S. Government Rights - Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements. Use is subject to license terms. This distribution may include materials developed by third parties.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and in other countries, exclusively licensed through X/Open Company, Ltd. X/Open is a registered trademark of X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, Java, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

This product is covered and controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical biological weapons or nuclear maritime end uses or end users, whether direct or indirect, are strictly prohibited. Export or reexport to countries subject to U.S. embargo or to entities identified on U.S. export exclusion lists, including, but not limited to, the denied persons and specially designated nationals lists is strictly prohibited.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Table of Contents

Introduction.....	4
Legacy Master Read Servicing Models.....	4
Limited Number of Servers.....	4
Applications Conducting Both Read and Write Operations.....	4
Enhanced Directory Server 6 Features for Write Operations.....	5
Write Referral Risk and Mitigation.....	5
Considerations for Directory Server 6 Multimaster Deployments.....	5
Directory Server 6 Consumer Directory Deployment Models (Read Only).....	6
Fractional Replication Consumer Directory Server Model.....	6
Highly Secured Consumer Directory Server Model.....	6
Lightweight Consumer Directory Server Model.....	6
Comparison of Exclusively Multimaster and Multimaster-to-Consumer Topologies.....	7
Example of Exclusively Multimaster Directory Server 6 Topology.....	9
For More Information.....	9

Introduction

One of the significant features of Sun Java™ System Directory Server Enterprise Edition 6 (hereafter referred to as "Directory Server 6") is that it allows unlimited master directory servers. This document describes the benefits of deploying an exclusively multimaster topology instead of a master, consumer, and replication hub directory topology.

Using an exclusively multimaster deployment provides the following benefits:

- Mitigates risk in isolating existing application write behavior
- Provides the greatest aggregate performance in a highly distributed and balanced model
- Lowers administrative burden in failover and recovery requirements

Customers using Directory Server 5.x masters for read traffic typically use one or more of the models described in this document. To define read and write operations, write operational traffic is considered to be any of the following:

- Creation of new directory objects (in a typical user model, creation of new users)
- Object modification (password, telephone, surname changes)
- Object deletion (user purging)

Read operational traffic is search operations (in a typical user model, authentications, authorizations, and entitlements).

Legacy Master Read Servicing Models

Limited Number of Servers

Customers can combine read and write traffic on the same physical servers. Typically, within the Directory Server 5.2 framework, this model is used to save in hardware costs. Services are potentially impacted during peak usage and maintenance. Degraded performance might occur for provisioning (write) applications during heavy read operation load and, alternatively, when heavier write demand impacts read or search availability.

Higher availability is generally not a key business requirement in these Directory Server 5.2 models.

Applications Conducting Both Read and Write Operations

This model is typically used in companies when there is limited knowledge of the behavior or capabilities of their business applications. These users might direct all operations to masters to avoid write referral requirements.

Application owners might independently direct new applications to the masters without the consent of the directory owners or administrators. These applications are sometimes identified only when observing directory server read operation statistics.

Bulk provisioning applications directed to the masters conduct minimal required read operations to manipulate target directory objects.

Within this model, multiple Directory Server 5.x Directory Proxy Server instances are sometimes deployed. One or more are designated for bulk provisioning applications using weighted or failover routing. The others are designated for everything else, including random writes distributed across a balanced routing table.

Enhanced Directory Server 6 Features for Write Operations

The following enhancements were introduced in Directory Server 6. They are specific to write operation performance and agility, and they should be considered during the architectural definition stage.

- Faster write acceptance
- Support for unlimited master directories
- Increased write speed by distributing write operations
- Write affinity ability
- Enhanced replication ability and speed
- Support for full and partially meshed replication topologies
- Increased management and administration of replication
- Operational-based routing ability
- Enhanced proxy routing based on availability
- Enhanced memory and cache management
- Global user lockout on failed password attempts

Write Referral Risk and Mitigation

Some Directory Server 5.x users experience risk related to applications and clients that are unable to effectively follow write referrals when write operations are requested from a consumer (read-only) directory server. This risk is mostly mitigated by using Sun Java System Directory Proxy Servers, because they can be defined to follow write referral requests on behalf of clients and applications. This transparent proxy operation is successful except for applications that do not generate the appropriate return codes. In these cases, a few options exist to mitigate risk; most involve small adjustments in the application code or the use of application environmental variables. Another mitigation that is used is to direct these specific applications and clients to master directory servers on which write referrals are not presented or required. Risk can be further mitigated by using Directory Server 6.

Directory Server 6 supports an exclusive multimaster architecture with unlimited masters, which can avoid write referral requirements because each master has the ability to accept localized write operations. The Directory Server 6 Directory Proxy Server also has the ability to direct write operations to the master directory servers. This ability can be defined according to design preferences, so a primary master can be thought of as the target or it can be routed using a balanced or weighted definition across the master directory servers. Directory Server 5.x also supports an exclusive multimaster architecture, but it supports a maximum of four multimaster directory servers.

Considerations for Directory Server 6 Multimaster Deployments

Full, exclusive use of master directory servers can be a deployment practice with Directory Server 6. Read-only consumer directories can be deployed only to address specific business requirements. A full master topology provides such high availability, increased aggregate performance advantages, and growth flexibility that read-only consumer directories might be less desirable and might be used only to fulfill specific business requirements.

Replication hubs, which are frequently used in Directory Server 5.x architectures, might be less significant in Directory Server 6 deployments. Support of full and meshed replication topologies and the enhanced management of replication agreements might make replication hub components less relevant and without cost advantage. Companies can replace the replication hub architecture in their legacy deployments with an additional multimaster directory to gain additional aggregate performance in a load-balanced strategy and also to provide additional unattended failover redundancy within their framework.

Synchronizing failed password attempts is achieved by writable master directory servers. Consumer directory servers can be leveraged in a failed-password, retry-count model when operational routing is used to direct authentications to masters. Comparisons between an exclusively multimaster model and a master-to-consumer model are provided later in this document.

Directory Server 6 Consumer Directory Deployment Models (Read Only)

Fractional Replication Consumer Directory Server Model

Fractionally replicated consumer directory servers provide directories that are deployed with a minimal set of user attributes in a read-only state, and these servers can be positioned in unsecured openly accessible areas (DMZs). In addition, these servers can be configured with fewer hardware requirements than the masters due to their limited data sets, potential for lower indexing and cache, and lack of a change log database.

Highly Secured Consumer Directory Server Model

Consumer directory servers are not capable of accepting write operations. These servers can be further protected by prohibiting indirect client or application writes by blocked write referrals when Directory Proxy Servers are used. Consistent protections can be provided in an exclusively multimaster deployment as well through options available within the Directory Proxy Servers and native directory server.

A typical use case for a restricted consumer read-only topology in which writes cannot be introduced, even indirectly by referrals, might be when the authoritative source of data exists in a back-end data repository pushed to the LDAP directory. Manipulation of data is never initiated within the LDAP architecture by LDAP clients or applications. The LDAP architecture in this model is basically a consumer of changes that are made from other data sources and pushed to the LDAP directory.

Lightweight Consumer Directory Server Model

Consumers can be deployed in a combined master-to-consumer model consistent with the Directory Server 5.x model. There is little gained in this two-directory-server-profile model (three profiles when replication hubs are used), and it includes a loss of some of the benefits gained in an exclusively master deployment. The emphasis in a consumer model, relative to performance, is typically to reduce directory server overhead by not maintaining a localized change log database. Read-only consumer directory servers do not maintain replication synchronization change logs.

A master-to-consumer or multimaster-to-consumer model can include Directory Server 6 operation-based routing or write referral handling through the Directory Server 6 Directory Proxy Services.

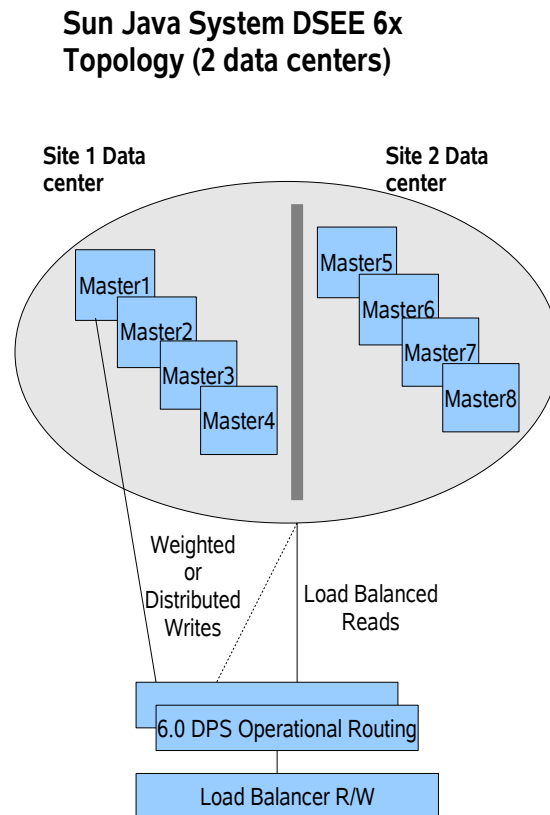
Comparison of Exclusively Multimaster and Multimaster-to-Consumer Topologies

	Exclusively Multimaster Topology	Multimaster-to-Consumer Topology
High Availability	Higher availability is realized because all masters can be configured consistently. Any master can be used to restore or initialize another master or build an additional master.	High availability is provided by redundancy within each of the server profiles, masters, consumers, and replication hubs. Greater hardware investment is typically required in definition of the different server profiles because redundancy and sustained service levels are required for each profile.
Aggregate Performance	When all exclusive master servers are configured consistently throughout and balanced through use of the Directory Server 6 Directory Proxy Servers, aggregate performance can be realized and grown inserting additional servers without any adverse service impact.	Having two or three profiles of servers, masters, and consumers, and potentially having replication hubs, and incorporating required redundancy within each of the profiles typically results in only similar servers being balanced and used for aggregate usage. There is greater likelihood that one profile or another will be less utilized, and aggregate performance potential from the whole architecture is not available.
Write Referrals and Localized Write Operations	All masters have the ability to accept localized writes and replicate these writes to other directory servers. No write referrals are required when only masters are used. This increases the speed of the write commitment because additional operational overhead is not required. Write affinity can also be leveraged so that immediate searches after writes are fulfilled successfully.	Only master directory servers are capable of accepting local writes. Consumer directories require write referral handling or operation-based routing to a master for write acceptance. Write referral handling and operation-based routing can be facilitated through the Directory Server 6 Directory Proxy Services.
Change Log Databases	<p>Change log databases exist only on master directory servers and are used to maintain replication synchronization to peer or subordinate servers.</p> <p>The advantage is that all masters can be identically configured and maintain synchronization. A master server can be restored or initialized quickly from another master and maintain quick synchronization based on the use of change log databases.</p> <p>A small disadvantage of having local change log databases on each master is the additional server disk write I/O. This disadvantage is mitigated by faster directory write capabilities in Directory</p>	<p>Change log databases exist only on master directory servers and are used to maintain replication synchronization to peer or subordinate servers.</p> <p>Consumers can be promoted to masters upon a recovery requirement but this requires administrative intervention, and a consumer might require significant time to establish itself as a master or peer with other servers.</p> <p>Best practices do not depend on consumer promotion to master strategies. The best practice master recovery model uses an alternate multimaster in an unattended</p>

	Exclusively Multimaster Topology	Multimaster-to-Consumer Topology
	Server 6 and by potentially having fewer servers than in a typical redundant master, redundant consumers model (that possibly also has replication hubs) and by having fewer but higher-performance servers.	failover. Best practice deployments include a minimum of three master directory servers for high availability of writes. Consumers without change log database write overhead consume less disk I/O.
Password Retry Lockout	Only writable servers (masters) are capable of maintaining and synchronizing the failed password attempts. Lockout state is replicated automatically regardless of whether the directory is a master or a consumer.	Only writable servers (masters) are capable of maintaining and synchronizing the failed password attempts, so when consumers are used, administrators can direct all authentication requests to the master servers and redirect to consumers their normal search and entitlement operations. This operation-based routing is available through the Directory Server 6 Directory Proxy Server. Lockout state is replicated automatically regardless of whether the directory is a master or a consumer.
Binary Backup and Restore	Binary recovery is supported only by “like” servers. A master with a consistent configuration can be used to initialize or recover another master server. Any master can be used in a consistent model.	Binary recovery is supported only by “like” servers. A master with a consistent configuration can be used to initialize or recover another master server. A consumer directory can be used only to initialize or recover another consumer directory server.
Hardware Requirements	Fewer servers can be defined in this architecture because each master can have a consistent definition and fulfill both read and write operations. New master servers can be included in aggregate use through proxy and load balancing.	Typically, more servers are used because specific servers are assigned to specific assignments. Adequate server redundancy is required for consumers and masters.
Replication Hub Requirements	Typically, in exclusive multimaster topologies, replication hubs are not required because flexible replication routing definitions across masters can be achieved.	Replication hubs might be required in some master-to-consumer topologies to offload master replication overhead to the subordinate consumer servers.
Load-Balanced Writes	Performance benchmark results indicate that Directory Server 6 enhanced collision avoidance and the speed of directory writes contribute to significant gains in distributing directory writes. Customer preference will dictate this write routing strategy and decisions can be made virtually on the fly between strategies within the Directory Proxy Server.	In a master-to-consumer model, only the masters accept the balanced or target writes. Not utilizing all servers as masters dictates that fewer masters are available than in an exclusive model, and this subsequently reduces the aggregate benefit realized in benchmarks distributing the write load.

Example of Exclusively Multimaster Directory Server 6 Topology

The following figure provides an example.



For More Information

Here are additional resources:

- Sun Java System Directory Server Enterprise Edition downloads: http://www.sun.com/software/products/directory_srvr_ee/get.jsp
- Java Enterprise Systems forums: <http://forum.java.sun.com/index.jspa?tab=es>

- Sun training courses at <http://www.sun.com/training/>:
 - Sun Java System Directory Server Enterprise Edition 6.x: Maintenance and Operations (DIR-2337D)
 - Sun Java System Directory Server Enterprise Edition 6.x: Analysis and Planning (DIR-2217)
 - Sun Java System Directory Server Enterprise Edition: LDAP Concepts (WMT-DIR-1344)
 - Sun Java Identity Management Suite: Integrated Solutions (SEM-IDM-1482 and WMT-IDM-1482)
- Support:
 - Register your system with Sun Connection: <http://www.sun.com/bigadmin/hubs/connection/>
 - Services: <http://www.sun.com/services>
 - SunSolve Online: <http://sunsolve.sun.com>
- Related documents at <http://docs.sun.com>:
 - Sun Java System Directory Server Enterprise Edition 6.2 documentation collection
 - Sun Java System Directory Server Enterprise Edition 6.1 documentation collection
 - Sun Java System Directory Server Enterprise Edition 6.0 documentation collection
- Sun Java System Directory Server wiki: <http://wikis.sun.com/display/SunJavaSystem/Sun+Java+System+Directory+Server>
- Related web sites and articles:
 - BigAdmin Sun Java Enterprise System hub: <http://www.sun.com/bigadmin/hubs/javaes/overview/index.jsp>
 - Sun Java System Directory Server Enterprise Edition web site: http://www.sun.com/software/products/directory_srvr_ee/index.jsp
- Events of interest to users of Sun products: <http://www.sun.com/bigadmin/hubs/comms/community/events.jsp>