

## **Exclusive DSEE6 Multi-Mastered Deployment Considerations**

Version: 1.3

© Sun Microsystems, Inc. All rights reserved., August 17, 2006

## Introduction

One of the rich features of the DSEE6 offering allows for unlimited master directory servers. The intent of this document is to provide benefits and considerations in deploying an exclusive multi-master topology in comparison to a master, consumer and replication hub directory topology.

Selection of an exclusive multi-mastered directory deployment

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

Customers utilizing their DS5.x master(s) for read traffic typically satisfy one or more of the following models. To qualify read and write operations, write operational traffic is considered new directory object creations (in a typical user model, new user creations), object modifications (password, telephone, surname changes), or object deletions (user purging). Read operational traffic is considered search operations (in a typical user model, authentications, authorizations, and entitlements).

## Legacy Master Read Operation Usage Models

### Limited Server Architectures

Customers may combine read and write traffic on the same physical server(s) typically within the DS5.2 framework, this model is used to save in hardware costs. Services are potentially impacted during peak usage and maintenance. Degraded performance may be realized to provisioning (write) applications during heavy read operation load, and alternatively when heavier write demand impacts read/search availability.

Higher availability is generally not a key business requirement in these DS5.2 models.

### Applications Conducting Read and Write Operations

Profiles in this model typically includes, customers with limited knowledge of the behavior or capabilities of their business applications and may direct all operations to masters to avoid write referral requirements.

Application owners may independently direct new applications to the master(s) without consent of the Directory owners/administrators. They are sometimes only identified when observing directory server read operation statistics.

Bulk provisioning applications directed to the Master(s) conduct minimal required Read Operations to manipulate target directory objects.

Within this model multiple DS5.x Directory Proxy Server instances are sometimes deployed, one or more designated for bulk provisioning applications utilizing weighted or fail-over routing, the other(s) designated for

everything else including random writes distributed across a balanced routing table.

## DSEE6 Rich Feature Set (specific to write operations)

A number of enhancements are introduced within the DSEE6 offering specific to Write Operational performance and agility, and may be considered during the architectural definition stage.

- Faster Write Acceptance
- Unlimited Master Directories Supported
- Increased Write Speed Realized by distributing Write Operations
- Write Affinity Ability
- Enhanced Replication Ability and Speed
- Support of 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 / Mitigation

Some DS5.x customers have experienced risk related to applications and clients unable to effectively follow write referrals when write operations are requested from a Consumer (read-only) directory server. This risk was mostly mitigated through use of Sun's Directory Proxy Server(s) as the Directory Proxy Server may be defined to follow write referral requests on behalf on clients and applications. This transparent proxy operation is successful except where some applications as written do not generate the appropriate return codes. In these cases a few options existed to mitigate this risk, mostly around small adjustments in the application code, or through application environmental variables. Another mitigation historically used is to direct these specific applications/clients to master directory servers where write referrals are not presented or required. This risk can be further mitigated within the DSEE6 offering.

DSEE6 supporting an exclusive Multi-Mastered Directory architecture with unlimited masters can avoid write referral requirements as each master will have the ability to accept localized write operations. The DSEE6 Directory Proxy Server also has the ability to direct Write Operations to the master directory servers. This may be defined according to design preference where a primary master may be thought of as the target or may be routed via a balanced or weighted definition across the master directory servers. DS5.x also supported an exclusive Multi-Mastered Directory architecture with a supported limit of 4 Multi-Mastered Directory servers.

## New DSEE6 Multi-Master Considerations

Full exclusive use of master directory servers will be a common deployment practice within DSEE6 use. It is expected that “Read Only” consumer directories may only be deployed addressing specific business requirements. A full master topology will provide such high availability, increased aggregate performance advantages and growth flexibility that it's expected read-only consumer directories may be less desirable and may only be utilized to fulfill specific business requirements.

It's expected that Replication Hubs frequently used within DS5.x architectures may become less significant in DSEE6 deployments. Support of full and meshed replication topologies and the enhanced management of replication agreements are likely to make Replication Hub components less relevant, and without cost advantage. Customers would likely replace this replication hub concept in their legacy deployments with an additional multi-master directory so as to gain additional aggregate performance in a load balanced strategy, and provide additional unattended fail-over redundancy within their framework.

Failed “password attempt counts” synchronization is achieved via writable Master Directory servers. Consumer directory servers may be leveraged in a failed password retry count model when operational routing is used directing authentications to Masters. Comparisons between exclusive master directory models and master to consumer models are indicated later within this document.

## Potential DSEE6 Consumer Directory Deployment Models - (read only)

### Fractional Replication Consumer Directory Servers

Directories deployed with a minimal set of user attributes, in a read only state, these servers may be positioned in unsecured openly accessible areas (DMZ's) . These fractionally replicated consumer directory servers may be configured with lower hardware requirements than the masters based on their limited data sets, potential for lower indexing and cache, and lack of a change log database.

### Highly Secured Consumer Consideration

Consumer directory servers are not capable of accepting write operations. These servers can be further protected by prohibiting indirect client/application writes via blocked write referrals when Directory Proxy Servers are used. Consistent protections can be provided in an exclusive master 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 where writes can not be introduced even indirectly via referrals, may be one where the authoritative source of data exists in a back-end data repository pushed to the LDAP directory. Manipulation of data will never be initiated within the LDAP architecture by LDAP clients or applications. The LDAP architecture in this model is basically a consumer of changes made from other data sources, pushed to the LDAP directory.

### Light Weight Consumer Consideration

Consumers may be deployed in a combined master to consumer directory model consistent with the past DS5.x

model. There is little gained in this two directory server profile model (three profiles when replication hubs are used), and includes a loss of some of the benefits gained in a full exclusive master deployment. The emphasis in a consumer model related 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 the replication synchronization change logs.

A master or multi-master to consumer model may include DSEE6 operational based routing or write referral handling via the new DSEE6 Directory Proxy Services.

## Comparison of Exclusive Multi-Master Topology and Multi-Master to Consumer Topology

	Exclusive Multi-Master Topology	Multi-Master / Consumer Topology
<b>High Availability</b>	Higher availability is realized as all masters may be consistently configured. Any master may be used to restore/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 as redundancy and sustained service levels are required for each profile.
<b>Aggregate Performance</b>	When all exclusive master servers are consistently configured throughout and balanced through use of the DSEE6 directory proxy servers aggregate performance can be realized and grown by insertion of additional servers without any adverse service impact.	Having two or three profiles of servers, masters and consumers and potentially replication hubs, and incorporating required redundancy within each of the profiles, only the like servers are typically balanced and utilized for aggregate usage. There is greater likelihood that one profiles or the other will be less utilized and aggregate performance potential from the whole architecture is not available.
<b>Write Referrals / Localized Write Operations</b>	All masters will 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 as additional operational overhead is not required. Write affinity may also be leveraged so that immediate searches after	Only master directory servers are capable of accepting local writes. Consumer directories require write referral handling or operational based routing to a master for write acceptance. Write referral handling and operational based routing can be facilitated via the DSEE6 directory

	Exclusive Multi-Master Topology	Multi-Master / Consumer Topology
	writes are fulfilled are successful.	proxy services.
<b>Change Log Database</b>	<p>Change log databases only exist 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. Master server can be restored or initialized quickly from another master and maintain quick synchronization based on the use of change log database.</p> <p>A small disadvantage of having local change log databases on each master is the additional server disk write I/O. This is mitigated by faster directory write capabilities in DSEE6 and potentially having less servers than typical in a typical redundant master, redundant consumers model and possibly replication hubs, and having less newer higher performance servers.</p>	<p>Change log databases only exist 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 requires administrative intervention and may require significant time to establish itself as a master or peer with other servers.</p> <p>Best practices are not to utilize a consumer in a promotion to master strategy. The best master recovery model utilizes an alternate multi-master as an unattended fail-over strategy. Best practice deployments include a minimum of 3 master directory servers for high availability of writes.</p> <p>Consumers without change log database writes will have less disk I/O.</p>
<b>Password Retry Lockout</b>	Only writable servers (masters) are capable of maintaining and synchronizing the failed password attempts. Lockout state is replicated automatically regardless of the directory being a master or consumer.	As only writable servers (masters) are capable of maintaining and synchronizing the failed password attempts, when consumers are used administrators may direct all authentication requests to the master server(s) and redirect to consumers their normal search/entitlement operations. This operational based routing is available via the DSEE6 directory proxy server. Lockout state is replicated automatically regardless of the directory being a master or consumer.
<b>Binary Backup / Restore</b>	Binary recovery is only supported by "like" servers. A master with a consistent configuration may be used to initialize/recover another master server. Any	Binary recovery is only supported by "like" servers. A master with a consistent configuration may be used to initialize/recover another master server.

	<b>Exclusive Multi-Master Topology</b>	<b>Multi-Master / Consumer Topology</b>
	master can be used in a consistent model.	A consumer directory can only be used to initialize/recover another consumer directory server.
<b>Hardware Requirements</b>	Less servers may be defined in the architecture as each master can have a consistent definition and fulfill both read and write operations. New master servers may be included into aggregate use through proxy / load balancing.	More servers are typically used as specific servers are assigned to specific assignments. Adequate server redundancy is required for consumers and masters.
<b>Replication Hub Requirement</b>	Replication Hubs in exclusive multi-master topologies are typically not required as flexible replication routing definitions across masters can be achieved.	Replication Hubs may be required in some master to consumer topologies to off load master replication overhead to the subordinate consumer servers.
<b>Load Balanced Writes</b>	Performance benchmark results indicate the DSEE6 enhanced collision avoidance and new speeds 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 will accept the balanced or target writes. Not utilizing all servers as masters dictates less masters available than an exclusive model and subsequently reduces the aggregate benefit realized in recent benchmarks distributing write load.

## An Exclusive Multi-Mastered DSEE6 Directory Topology

### LDAP V6.0 “Strawman” Topology (2 datacenters)

