

# A Technical Overview of the Sun™ ONE Directory Server 5.2

White Paper  
July 2003



# Table of Contents

<b>Introduction</b> .....	<b>.1</b>
What Is a Directory Service? .....	1
<b>The Sun ONE Directory Server Architecture</b> .....	<b>.3</b>
Components of the Sun ONE Directory Server .....	3
Architecture Overview .....	4
Overview of the LDAP and DSMLv2 Front Ends .....	4
Extensibility Through Plug-ins .....	4
Directory Information Tree .....	5
<b>Key Features</b> .....	<b>.6</b>
Support for Industry Communication Standards .....	6
LDAP Version 3 .....	6
DSML Version 2 .....	7
Highly Advanced Architecture .....	7
Multiplatform Support .....	7
Multidatabase Design .....	8
Large Cache Support .....	8
Improved Update Performance .....	8
Improved Search Performance .....	8
Use of the Sun Cluster 3.0 Agent Module .....	9
Advanced Replication Features .....	9
Efficient Searching Using Indexes .....	13
Advanced Security Features .....	14
Multiple Password Policy .....	14
Controls for Resetting Passwords .....	14
Attribute Encryption .....	14
SSL Encryption and Authentication .....	15
Start Transport Layer Security .....	15
SASL Encryption and Authentication .....	15
Retrieval of Effective Rights .....	16
Support for the Sun Crypto Accelerator 1000 Board .....	16
Fractional Replication for Security .....	16
Identity Synchronization for Windows .....	16
Flexible Administration .....	17
Roles and Class of Service .....	17
Tools for Migrating From Previous Versions .....	18
Enhanced Server Management Console .....	18
On-the-Fly Schema Changes .....	18
<b>Additional Resources</b> .....	<b>.19</b>

## Chapter 1

# Introduction

The Sun™ ONE Directory Server 5.2 is a powerful, scalable, distributed directory server based on industry standards, the Lightweight Directory Access Protocol (LDAP), and the Directory Services Markup Language (DSML). Part of the Sun Open Net Environment (Sun ONE), the Sun ONE Directory Server provides the foundation for the new generation of e-business applications and Web services, with a centralized and distributed data repository that can be used in an intranet or over an extranet with trading partners.

## What Is a Directory Service?

A directory provides a network service for the management of information about an enterprise, typically including data on computers, other network services, equipment, users, employees, customers, and subscribers. Although a directory service can be considered a type of database, directory services have several important characteristics that make them particularly well suited for this function. These characteristics include a hierarchical object-oriented naming model, extensive search capabilities, an extensible schema, built-in attribute-level security, shared network access, replication for increased performance and high availability, and an underlying storage mechanism optimized for the requirements of network services.

The directory protocol and data models are designed to allow multiple applications — those developed by Sun, other software providers, and in-house developers — to share a common data repository. LDAP and DSML over HyperText Transfer Protocol (HTTP)/Simple Object Access Protocol (SOAP) access protocols enable clients anywhere on a network to securely search, update directory data objects, receive changes made by other applications, and authenticate users or applications.

Online directories that support LDAP have become critical components of the corporate and e-business infrastructure. LDAP directories can be configured to use the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocols for authenticated and encrypted communications.

The Sun ONE Directory Server provides global directory services, meaning it provides information to a wide variety of applications. Rather than using proprietary databases for each application, the Sun ONE Directory Server employs a global directory service that provides a single, centralized repository of directory information that any application can access, as well as two standard protocols that applications can use to access its directory: LDAP and DSML.

## Chapter 2

# The Sun ONE Directory Server Architecture

This section describes the components installed with the Sun ONE Directory Server 5.2 and provides an overview of the Sun ONE Directory Server architecture.

## Components of the Sun ONE Directory Server

Along with the directory server itself, the Sun ONE Directory Server includes a set of tools for data and directory administration through APIs, command-line interfaces, and graphical user interfaces. Other directory client programs can be purchased, or programs can be written using the LDAP client SDK provided with the Sun ONE Directory Server or using XML. Operating systems, such as the Solaris™ 9 Operating System (OS), can also leverage the directory server for activities such as authentication.

When the Sun ONE Directory Server is installed, the following components are installed on the system:

- An extensible directory server (Sun ONE Directory Server) with both LDAP and DSMLv2 over SOAP front ends
- The Sun ONE Administration Server to enable remote management
- The Sun ONE Server Console to manage the servers through the graphical user interface
- Command-line tools for starting and stopping the server, importing and exporting data in the database, reindexing the database, inactivating and reactivating accounts, backing up and restoring, and performing LDAP Data Interchange Format (LDIF) merges

- A Simple Network Management Protocol (SNMP) agent
- A set of tools for migrating from previous versions of the Sun ONE Directory Server
- A set of clients tools

## Architecture Overview

At installation, the Sun ONE Directory Server contains the following:

- The core server, responsible for processing requests
- The Sun ONE Directory Server Console, the graphical user interface for managing the directory server
- Front ends responsible for LDAP, DSMLv2, and SNMP
- Plug-ins for server functions, such as access control and replication
- An initial directory information tree, consisting of server configuration and sample enterprise data

The following sections describe the components of the directory in more detail.

### Overview of the LDAP and DSMLv2 Front Ends

The Sun ONE Directory Server supports any standards-based client, using either LDAP over TCP/IP or DSMLv2 over HTTP/SOAP.

Multiple clients can bind to the server at the same time over the same network because the Sun ONE Directory Server is a multithreaded application. As the directory services grow to include larger numbers of entries or larger numbers of clients spread out geographically, multiple Sun ONE Directory Server systems can be included, placed in strategic places around the network or organization. Directory servers can also be distributed to conform with data protection regulations as well as to provide high availability.

### Extensibility Through Plug-ins

The Sun ONE Directory Server relies on plug-ins for many key features. A plug-in is a way to enable, configure, and add functionality to the core server. For example, plug-ins are included to support referential integrity and uniqueness constraints.

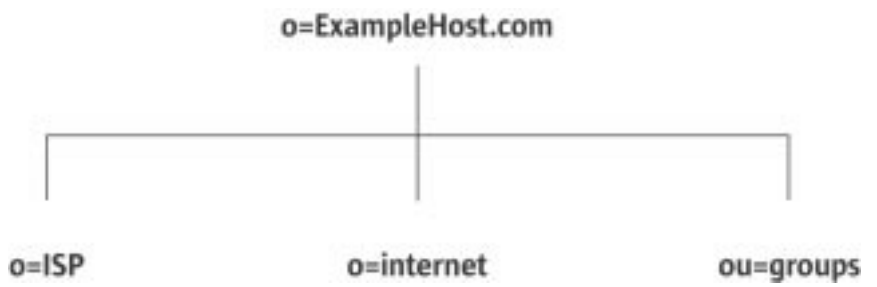
Plug-ins extend the Sun ONE Directory Server by adding pre- or post-operational functionality. New intelligence can be added to operations, providing the ability to adapt the directory to other applications, changing business requirements, the needs of partners, and so on.

The plug-in API is fully documented in this release of the Sun ONE Directory Server, enabling the creation of custom plug-ins. In addition, Sun Services and other organizations can provide assistance in developing custom plug-ins. For more information, contact Sun Services at the addresses given at the end of this document, or contact your local Sun support representative.

### Directory Information Tree

The Sun ONE Directory Server contains a basic directory information tree (DIT) at installation time. This tree mirrors the tree model used by most file systems, with the tree's root, or first entry, appearing at the top of the hierarchy. Figure 2-1 illustrates an example of the basic directory information tree. This tree can be built to add any data relevant to a directory installation.

Figure 2-1: Basic directory information tree



## Chapter 3

# Key Features

This section describes in detail the key features provided with the Sun ONE Directory Server 5.2 designed to help customers deploy extensible, secure, highly available, global directory services.

## Support for Industry Communication Standards

The Sun ONE Directory Server 5.2 supports two standard communication protocols: LDAP version 3 and DSML version 2.

### **LDAP Version 3**

The Sun ONE Directory Server supports LDAP versions 3 (RFC 2251), the definitive Internet Proposed Standard protocol for accessing directory information. LDAP was invented by the University of Michigan, and the Sun ONE Directory Server is based on this original University of Michigan LDAP code.

LDAP provides a common language that client applications and servers use to communicate with one another. LDAP applications can easily authenticate, search, add, delete, and modify directory entries.

The Sun ONE Directory Server supports LDAP search filters as outlined in RFC 2254, including: presence, equality, inequality, substring, approximate match (for phonetic matching), greater than, less than, and Boolean combinations of the previous filters using the and (&), or (|), and not (!) operators.

The Sun ONE Directory Server supports LDAP version 3 search references (also known as smart referrals), which allow the directory to refer a query to another directory. The Sun ONE Directory Server also implements LDAP URL formats as outlined in RFC 2255, and uses the LDAP Data Interchange Format (LDIF) for exchanging directory information (RFC 2849).

### **DSML Version 2**

DSML is a markup language that enables directory entries and commands to be represented in XML. The Sun ONE Directory Server implements version 2 of the DSML standard (DSMLv2). DSML enables developers to combine the power of XML in presenting and manipulating data with the scalability, security, availability, and information management strengths of the Sun ONE Directory Server.

Because DSML is not an access protocol, the Sun ONE Directory Server uses HTTP and SOAP version 1.1 to transport the DSML content. The Sun ONE Directory Server supports DSML natively, providing very high throughput performance as opposed to the gateway design used with other LDAP directories.

By using DSML over HTTP/SOAP, applications can be created that do not rely on LDAP, allowing non-LDAP clients to interact with directory data. The Sun ONE Directory Server DSML front end also interoperates with the DSML implemented by other product vendors. This allows the creation and implementation of a new generation of Web services that interface with the directory server through XML.

The DSML front end of the Sun ONE Directory Server is a restricted HTTP server because it accepts only DSML HTTP post operations and rejects requests that do not conform to the SOAP/DSML specification. Because the DSML front end is a core component of the directory, all native access controls apply. As a result, any and all security rules previously defined for LDAP also apply to DSML, including simple authentication, SSL authentication, and access control instructions (ACIs).

## **Highly Advanced Architecture**

The Sun ONE Directory Server 5.2 is based on an advanced architecture that includes multiplatform support, multidatabase design, large cache support, improved update performance, improved search performance, use of the Sun Cluster 3.0 agent module, advanced replication features, and indexes for fast searches.

### **Multiplatform Support**

The Sun ONE Directory Server 5.2 supports the following platforms: Sun Solaris 8 OS for UltraSPARC® (32- and 64-bit) systems, Sun Solaris 9 OS for SPARC® (32- and 64-bit) systems, Sun Solaris 9 OS for x86 (IA-32) systems, Microsoft Windows 2000 Server and Advanced Server SP 3 (IA-32), Red Hat Linux 7.2 (IA-32), Sun Linux 5.0 (Sun LX50), Hewlett-Packard HP-UX 11.i PA-RISC 1.1 or 2.0 (32- and 64-bit), and IBM AIX 5.1 (PowerPC) (32-bit).

This support of multiple platforms means that a directory solution can be built using current platform choices, preserving an enterprise's investment in hardware and software.

With nearly two billion users, the Sun ONE Directory Server has a proven history of high stability and performance.

Installation of the Sun ONE Directory Server is very similar across platforms. The installer includes a wizard, or the software can be installed using the command-line utilities. Both Solaris package installation and traditional compressed archives are provided.

The silent installation can be used to install the software automatically without any user input. This feature is useful for installing large deployments with many instance across multiple sites.

### **Multidatabase Design**

The multiple database architecture of the Sun ONE Directory Server supports distributed naming contexts, providing large scalability to support millions of users on a single system, improved backup and restore, load balancing, and simplified administration. The multidatabase design also provides a method for partitioning the directory data to simplify replication.

### **Large Cache Support**

The Sun ONE Directory Server 5.2 can run as a 64-bit application on Solaris SPARC and HP-UX systems. This means that the Sun ONE Directory Server can use a cache larger than the 4-GB limit of 32-bit applications. Because caching is a critical means of tuning the Sun ONE Directory Server, using the large cache allows better performance to be attained for high-volume deployments. The size of the cache scales to the limits of the bandwidth, meaning the only limit is the size of the machine.

### **Improved Update Performance**

The Sun ONE Directory Server 5.2 incorporates several enhancements, including:

- **Group flush.** The Sun ONE Directory Server can be configured to increase the speed of update operations by waiting for several operations to be completed before writing them to the physical disk and sending the acknowledgment back to the client application. Usually, when an update is made, the modified data is written to the physical disk device. However, writing to disk has a higher latency than writing to memory. Hardware such as the Sun StorEdge™ T3 Array, which includes an extra level of cache to improve write performances, can be used.
- **Index compression.** The index compression enhancement improves performance on large databases with large index lists and does not require specific configuration.
- **Replication compression.** On Solaris and Linux systems that communicate over a WAN, replication can be compressed to maximize the throughput on the WAN connection. This feature automatically optimizes bandwidth usage on the WAN and speeds up replication.
- **Improved checkpointing.** Checkpoints and updates are now carried out in parallel.

### **Improved Search Performance**

The Sun ONE Directory Server 5.2 incorporates the following search performance improvements:

- **64-bit server process.** The entry, database, and import caches can now all be simultaneously larger than 4 GB. This means that the process size is no longer a concern. With the increased cache size, searches now scale almost linearly on servers with up to 12 processors.
- **Improved algorithm for reading from the database cache to the entry cache.** Performance is improved through reduced memory allocation and improved thread management.

### Use of the Sun Cluster 3.0 Agent Module

The Sun Cluster agent module is a high availability agent that provides LDAP service failover. It is bundled with the Sun ONE Directory Server, with a goal of providing 99.95% availability to Sun ONE Directory Server data services.

With Sun Cluster software, although one backup node is offline, the software constantly checks the viability of the primary node. If it does not respond, the backup node takes over the IP identity of the original node, responding to operations requests. This feature is useful for directories that support large populations with strict availability requirements, such as large banks or telecommunication companies.

### Advanced Replication Features

The Sun ONE Directory Server supports simple, cascading, and multi-master replication, all of which ensure the high availability of directory services for both read and write operations. An additional replication feature, called fractional replication, provides content security.

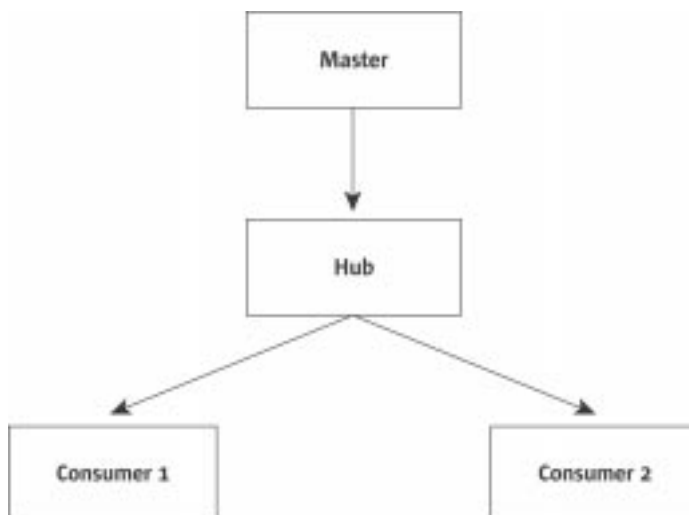
The Sun ONE Directory Server replication protocol defines two roles that help to understand the features described in this section:

- The supplier, which is the server that sends the updates
- The consumer, which is the server that receives the updates

#### *Cascading Replication*

In cascading replication, the Sun ONE Directory Server acts as a hub supplier. A hub is a read-only database, similar to a consumer replica. However, a hub also accepts replication from one or more master servers and replicates the changes to consumer servers. Figure 3-1 illustrates a basic cascading replication scheme.

**Figure 3-1:** Cascading replication scenario



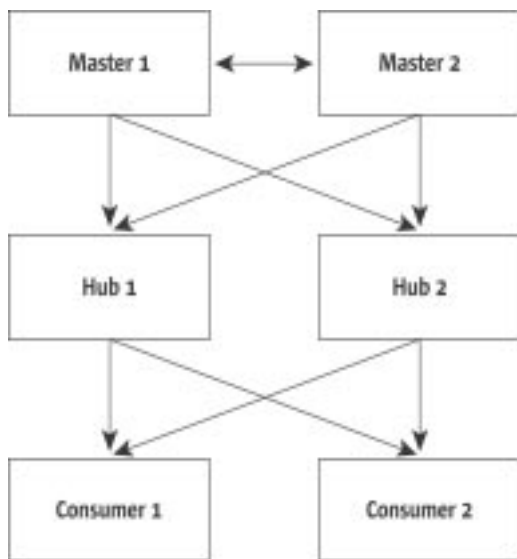
In a regular replication scenario with one master and many consumers, the master's resources are consumed by replicating information. Using cascading replication, the master concentrates on handling operations, while the hub handles replicating data to all of the consumers.

Cascading replication can be used to balance heavy traffic loads, reduce connection costs with local hubs in a geographically distributed environment, and increase performance. Using cascading replication, the use of hardware resources can be optimized.

A cascaded architecture can be tuned so that it optimizes the indexes, logs, cache size, and so on of a directory server. For example, the indexes on each server can be optimized so that there is an update index for the Supplier, a common name index for Consumer 1, and a phone number index for Consumer 2.

### Multi-Master Replication

The Sun ONE Directory Server 5.2 supports four-way multi-master replication over wide-area networks (WANs). When combined with simple and cascading replication scenarios, multi-master replication provides a highly flexible and scalable replication environment for enterprises and service providers with global data center operations. Figure 3-2 illustrates a multi-master and cascading replication scheme.



**Figure 3-2:** Multi-master and cascading replication scenario

In multi-master replication, a master replica is available on up to four Sun ONE Directory Server systems. A master replica is a read-write database that contains a master copy of the directory data. Each master acts as a supplier and a consumer to the other Sun ONE Directory Server systems.

Four-way multi-master replication is ideal for distributed deployments. For example, an enterprise could establish two masters in San Francisco and two masters in New York. If something happened to both of the masters at a single location, the two masters at the other location can continue to provide the service.

Multi-master deployments provide 24x7 service levels with write failover. For example, if one server fails, the others remain available for writes. When the server comes back online, it receives replication updates from the other masters.

The multi-master replication protocol is streamlined, enabling:

- Replication of updates based on the replica ID. The replica ID makes it possible for a consumer to receive updates for different replica IDs from multiple suppliers at the same time, improving performance.

This method also ensures the replication of only the updates that come from a replica ID for which the supplier and consumer are not yet synchronized. Only one supplier can replicate changes for a replica ID at a given time for a particular consumer.

- A replication agreement to be enabled or disabled with a particular consumer, providing more flexibility in configuring how to deploy replication. For example, this feature can be used to configure a fully connected topology and use only part of it.

A replication agreement can be enabled or disabled remotely for a particular consumer by modifying a single attribute value. By default, replication agreements are enabled.

A fully connected, four-way multi-master replication topology helps guarantee replication even if one or more masters fail. This type of deployment is appropriate for systems that have stringent availability requirements.

Multi-master replication uses a loose consistency replication model. This means that the same entries can be changed on different servers. When replication occurs between the two servers, the conflicting changes need to be resolved. Resolution occurs automatically, based on the timestamp associated with the change on each server.

When two entries are created with the same distinguished name (DN) on different servers, during replication the automatic conflict resolution procedure renames the last entry created by including the entry's unique identifier in the DN. Every directory entry includes a unique identifier given by the operational attribute `nsuniqueid`. If a naming conflict occurs, this unique ID is appended to the non-unique DN. Conflicting entries are marked by the attribute `nsds5replconflict` and are easy to search for.

#### *High Replication Performance*

The following enhancements can be used to ensure best performance on a LAN or WAN:

- Reduced latency by reducing the round-trip delay time using a special window mechanism. This mechanism allows the supplier to send multiple replication operation requests at once and then wait for an acknowledgment from the consumer before sending a new set of replication operation requests.
- Improved bandwidth performance by reducing the amount of data sent over the wire through smart compression and other internal enhancements.

#### *Replication Over WAN*

The replication mechanism of the Sun ONE Directory Server enables the distribution of directory databases across machines or network boundaries. Multi-master replication further allows geographical boundaries to be crossed, enabling large deployments over a WAN.

New features of the Sun ONE Directory Server ensure high performance, reliability, and security, despite the following replication challenges introduced by the WAN:

- Higher latency
- Lower bandwidth
- A potentially higher number of errors (such as disconnections, packet loss, packets out of order, and congestion)

Performance enhancement for multi-master replication ensure that replication works without seriously reducing network resources available for other directory operations.

*Fractional Replication*

In the Sun ONE Directory Server 5.2, fractional replication allows a subset of attributes to be replicated for all the entries in a given database. This filtering functionality can be valuable in replication environments where Sun ONE Directory Server systems are separated by WANs.

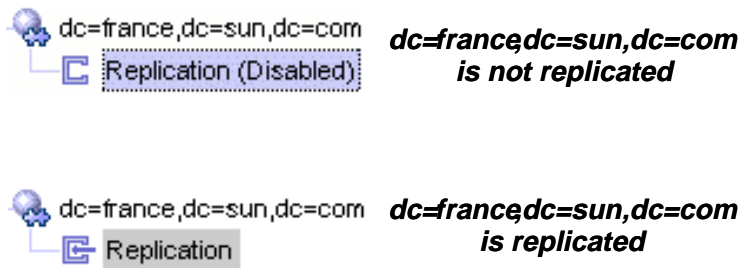
Fractional replication is described in detail in “Advanced Security Features” on page 14.

*Simplified Administration Through a New User Interface*

The Sun ONE Directory Server 5.2 Console offers a user-friendly way to configure replication. It also provides information about the status of replication.

In the Console, each suffix node has a replication node attached. An icon next to the node indicates if the suffix is replicated, as described in Figure 3-3.

**Figure 3-3:** Replication nodes in the Sun ONE Directory Server Console



When a replication node under a suffix in the Sun ONE Directory Server Console is selected, its contents provide different options depending on the state of the suffix, as illustrated in Figure 3-4.



**Figure 3-4:** Replication panel on the Configuration Tab

The Sun ONE Directory Server Console also provides a wizard for automatically creating replication agreements.

*Replication Discovery and Monitoring Tools*

The Sun ONE Directory Server provides replication management tools that allow monitoring of replication between servers. These tools simplify administration, particularly for complex directory server architectures, and can help users avoid errors.

The tools available are *insync*, *entrycmp*, and *repldisc*. In addition, new attributes have been added to the replication agreement entry to help identify the changes that have been sent to a consumer.

**insync:** The `insync` tool checks to determine if a master replica is synchronized with one or more consumer replicas. This tool helps in managing potential conflicts between suppliers or even whole servers.

The `insync` tool compares the replica update vector (RUV) of the supplier to the consumer. It then prints the time difference between the maximum change sequence numbers (CSNs).

**entrycmp:** The `entrycmp` tool compares a replicated entry to a copy of the entry on the consumer or master. The entries are considered equal if they have the same `nsuniqueid` value, the same number of attributes (as discovered using `ldapsearch`), or the same values for each attribute.

**repldisc:** The `repldisc` tool discovers a replication topology. The tool starts with one server and builds a graph of all the known servers within the topology. This tool is useful for managing large, complex deployments.

### Efficient Searching Using Indexes

The Sun ONE Directory Server implements indexes so that data in a directory can be searched quickly. The index files are stored in the directory's databases. The Sun ONE Directory Server supports the following types of indexes:

- **Presence index.** This index includes a list of the entries that contain a particular attribute. For example, this type of index can be used for examining any entries that contain access control information.
- **Equality index.** This index is for searching efficiently for entries containing a specific attribute value.
- **Approximate index.** This index allows efficient approximate searches. For example, a search against `locality~=San Francisco` (note the misspelling) would return entries including `locality=San Francisco`.
- **Substring index.** This index allows efficient searching against substrings within entries.
- **International index.** This index speeds up searches for information in international directories. During a search operation, it can be requested that the directory sort the results based on any language for which the server has a supporting collation order. The international index associates the object identifier (OID) of a locale with the attribute to be indexed.
- **Browsing (virtual list view) index.** This index speeds up the display of entries in the Sun ONE Directory Server Console. The browsing index displays entries in an order that can be configured, presenting them as small groups rather than as a large, unorganized list. A browsing index can be created on any branch of the directory tree to improve the display performance.

Separate, specialized indexes can be used for masters and consumers in a replication scenario. For example, a master replica might contain a UID index; a series of consumers that are used for phone number look-ups might contain a phone number index; another consumer series might contain an e-mail address index; while replication hubs might contain only system indexes.

The use of separate indexes helps ensure that each machine has indexes that are optimized for its role in the overall directory architecture.

## Advanced Security Features

The Sun ONE Directory Server provides a number of advanced security features, including fine-grained multiple password policies, controls for resetting passwords, attribute encryption, SSL encryption and authentication, Start Transport Layer Security (Start TLS), SASL encryption and authentication, effective rights retrieval, Sun Crypto Accelerator 1000 board support, content security through fraction replication, and identity synchronization using an additional module for Windows.

### Multiple Password Policy

With the Sun ONE Directory Server 5.2, multiple password policies can be configured and assigned either to particular users or to entire sets of users using class of service and roles. This flexible password policy scheme allows password policies to be created that meet security requirements for specific users or roles.

Multiple password policies are implemented using LDAP subentries. Password policies are identified through `passwordPolicySubentry` attributes on individual entries or on classes of entries using class of service or roles. By employing class of service and roles, password policy definitions can be shared by an arbitrary group of entries, allowing particularly flexible password policy assignments.

For example, an ISP decides it needs three password policies. Clients have passwords that never need to be changed. Internally, employees have passwords that they must change every month. Administrators, however, have to change their password every week, and the password must be 8 characters in length. Using the multiple password policy feature, each of these policies can be assigned to users using roles and class of service.

The design of the password policy provides maximum flexibility for adapting the Sun ONE Directory Server to the needs of a business model.

### Controls for Resetting Passwords

Passwords can be reset using a new modification request control that checks an ACI to confirm that the client binding to the directory is allowed to make the change. The directory manager can configure an administrator group with members who have the appropriate privileges to update passwords.

### Attribute Encryption

The Sun ONE Directory Server 5.2 supports the encryption of all attributes in the database, helping protect more than just the hashed `userPassword` attribute. The Sun ONE Directory Server 5.2 provides a powerful set of encryption algorithms: DES, Triple-DES, RC-Z, and RC-4. To increase the security of data, these algorithms can be used across different platforms to encrypt and decrypt attributes on disk.

Encryption uses the private key of a certificate to generate the key. The certificate and its private key are stored in a security token that is secured by a password or personal identification number (PIN). Users need to authenticate themselves to the security token to use the encrypted attribute.

Attribute encryption is transparent to users, who can perform LDAP operations without being aware of encryption. However, they can also export data that remains encrypted. For example, two servers might share the same certificate. The data can be encrypted, allowing the servers to share secure files for updates.

On a running server, authentication takes place when the server starts and remains valid for all directory operations performed on the data. Users must have the token PIN to perform both import and export operations whenever encrypted attributes are concerned.

Attribute encryption provides the highest level of security, protecting directory data from anyone in the enterprise, including administrators and operators.

### **SSL Encryption and Authentication**

The Sun ONE Directory Server supports LDAPS, the standard LDAP protocol that runs on top of SSL. SSL provides encrypted communications and optional authentication between the Sun ONE Directory Server and its clients.

SSL may be enabled for both the LDAP and DSML/HTTP protocols to provide security for any connection to the server. An SSL connection can be used to bind to the server in combination with certificate-based authentication, providing higher levels of security than password checks alone. Replication can also be configured to use SSL for secure communications between servers, preventing anyone from snooping data.

The Sun ONE Directory Server is capable of simultaneous SSL and non-SSL communications on separate ports. For security reasons, all communications to the secure port may also be restricted.

### **Start Transport Layer Security**

The Sun ONE Directory Server supports the Start Transport Layer Security (Start TLS) extended operation to enable TLS on an LDAP connection that was originally not encrypted. Start TLS is supported on Microsoft Windows and UNIX® platforms.

Start TLS allows a secure connection even if there is no dedicated encrypted port. A secure connection can be opened over the regular LDAP port.

### **SASL Encryption and Authentication**

The Sun ONE Directory Server 5.2 supports authentication and encryption using the Simple Authentication and Security Layer (SASL). The SASL mechanism is responsible for authenticating a user through SASL credentials.

On Solaris systems, the Sun ONE Directory Server supports the Generic Security Services API (GSSAPI) over SASL. The GSSAPI allows the use of a third-party security system such as Kerberos version 5 to authenticate clients. The server uses this API to validate the identity of the user. Then, the SASL mechanism applies the GSSAPI mapping rules to obtain a DN, which is the bind DN for all operations during this connection.

Client authentication may also be performed using DIGEST-MD5, a SASL-based mechanism of authenticating clients by comparing a hashed value the client sends with a hash of the user's password. Because the mechanism must read user passwords, a reversible encryption method must be used for the passwords of all users who want to be authenticated through DIGEST-MD5, or these passwords must be stored in the directory in clear text.

SASL provides advanced security, allowing the Sun ONE Directory Server to adapt to the security standards already established within an enterprise.

### **Retrieval of Effective Rights**

The Sun ONE Directory Server provides a new LDAP control that lets administrators and clients retrieve their access rights to directory entries and attributes. This feature is particularly useful for administering users, verifying access control policies, and debugging access control policy. This control is supported by the Sun ONE Directory Server Console and by LDAP search.

For example, if an access control policy consists of 20 access control instructions, to check that a particular role is giving the user the correct rights, an administrator can use the effective rights control.

When using the control, administrators specify the distinguished name (DN) of the user for which they want to know the effective rights, as well as any additional attributes. The control returns a rights attribute for each entry attribute returned.

For example, an application with a GUI can retrieve users rights and then modify the options it presents to a particular client (by graying out any options they do not have access to, such as writing).

### **Support for the Sun Crypto Accelerator 1000 Board**

The Sun ONE Directory Server 5.2 supports the use of the Sun Crypto Accelerator 1000 board. When using SSL, the Sun Crypto Accelerator 1000 speeds up the initial exchange of keys by performing specific SSL mathematical functions, leaving the system processor to focus on application processing. The Sun Crypto Accelerator 1000 does not speed up the encryption itself.

### **Fractional Replication for Security**

Fractional replication enables the replication of a subset of attributes by filtering out content for security reasons during the synchronization of intranet and extranet servers. For example, it might be necessary to replicate data to a directory server in a partner's network, but without duplicating the manager attribute, which exposes internal hierarchy. Fractional replication can hide this attribute, ensuring the partner receives only the information of interest to them.

Fractional replication can also help in complying with European Union data sharing regulations. A fractional replication scheme can be configured by specifying the list of attributes to include or by specifying the list of attributes to exclude, then activate the fractional replication scheme by modifying a single attribute value. Anytime the configuration of fractional replication is changed, consumers no longer contain the appropriate settings, so a replication restart is forced.

Checksums computed on the supplier side detect any changes to the configuration. Checksums retained on the consumer side ensure that replicated information comes only from suppliers that appear in the correct checksum.

The Sun ONE Directory Server configuration framework is conceived to ease the support of later partial replication features, including subtree and sparse replication.

### **Identity Synchronization for Windows**

Sun ONE Identity Synchronization for Windows software enables passwords to be synchronized on the Sun ONE Directory Server with Windows 2000 Active Directory and Windows NT. Users can change passwords in their native environments. All changes made on Windows NT will be automatically propagated to the Sun ONE Directory Server and vice versa. All error and change logs can be centralized to simplify the auditing process.

Nothing needs to be installed on a Microsoft Windows machine for synchronization between Windows 2000 Active Directory and the Sun ONE Directory Server. However, the software must be installed for synchronization with Windows NT.

This module runs on the Solaris 8 and 9 Operating Systems and Windows 2000/NT.

## Flexible Administration

The Sun ONE Directory Server provides the following features for flexible administration: roles and class of service, tools for migrating from previous versions, an enhanced server management console, and on-the-fly schema changes.

### Roles and Class of Service

The Sun ONE Directory Server delivers two features to ease identity and relationship management in large directory deployments: roles and class of service. Roles are an entry grouping mechanism. Role members can be specified either explicitly or dynamically depending upon the type of role being used (managed, filtered, or nested). Roles simplify application development by allowing applications to query either the members of a role or the roles held by a user without needing to know how the role members are specified.

With roles, the directory server does the work of computing role membership using the `nsRole` attribute. This attribute contains the DN of all role definitions in which the entry is a member. Roles also have a notion of scope within the directory tree, meaning that membership tests can be optimized for only the section of the directory of interest.

Roles are preferable to groups to enumerate members of a given role and find all role membership for a given entry. This is because the information is stored with the user entry, where it can be cached to make subsequent membership tests more efficient. The server performs all computations and the client only needs to read the values of the `nsRole` attribute. In addition, all types of roles appear in this attribute, allowing the client to process all roles uniformly.

Roles also form the basis of other Sun ONE Directory Server functionality. They can be used in resource-oriented access control instructions, as a basis for class of service, as part of more complex search filters, in defining password policies, and for activating and inactivating accounts.

Class of service enables sharing attributes between entries in a method that is transparent to applications and services. With class of service, some attribute values need not be stored with the entry itself. Instead, they are generated by the class of service logic as the entry is sent to the client application. For the application, these attributes appear just like all other attributes.

Roles and class of service can be used together to provide role-based attributes. These attributes appear on an entry because it possesses a particular role. For example, a role-based attribute could be used to set the mail quota for premium users and regular users.

Roles and class of service also form the basis of other server functionality, such as password policies, setting resource limits, and inactivating user accounts.

The Sun ONE Directory Server 5.2 now makes it possible to specify the attributes generated by roles and class of service in a search filter, returning the correct results in a timely manner. These attributes are not stored with the entry itself, but are returned to the client application along with the normal attributes in operation results.

### Tools for Migrating From Previous Versions

The Sun ONE Directory Server 5.2 provides a script for migrating data from versions 4.x and 5.x. Directory data and schema are automatically migrated. Replication agreements are automatically migrated from 5.x to 5.2.

**Enhanced Server Management Console**

Most administrative tasks can be performed from the Sun ONE Directory Server, such as adding and finding entries, updating schema, creating and managing groups and roles, creating classes of service, creating and managing access control instructions, inactivating user accounts or domains of accounts, creating replication agreements, and enabling replication.

Administrative tasks can also be performed with the command-line utilities provided with the Sun ONE Directory Server.

The Sun ONE Directory Server Console also provides support for the assistive software and technologies that make software accessible to users with disabilities.

**On-the-Fly Schema Changes**

The Sun ONE Directory Server comes with a standard schema that includes hundreds of object classes and attributes. Schema can also be extended by creating new object classes and attributes.

The Sun ONE Directory Server Console or basic LDAP modify commands (either from the command line or from an LDAP-enabled application) can be used to modify the schema.

The Sun ONE Directory Server also includes a schema checking function that ensures the object classes and attributes being used are defined in the directory schema, that the attributes required for an object class are contained in the entry, and that only attributes allowed by the object class are contained in the entry (avoiding any resulting inconsistencies).

## Chapter 4

# Additional Resources

For more information about the Sun ONE Directory Server, refer to the product documentation available on [docs.sun.com/coll/S1\\_DirectoryServer\\_52](http://docs.sun.com/coll/S1_DirectoryServer_52). This site includes the following documents, delivered in both HTML and PDF formats:

- *Sun ONE Directory Server 5.2 Getting Started Guide*: Provides a quick look at the key features of the Sun ONE Directory Server 5.2
- *Sun ONE Directory Server 5.2 Deployment Guide*: Explains how to plan the directory topology, data structure, security, and monitoring, and also includes example deployment scenarios
- *Sun ONE Directory Server 5.2 Installation and Tuning Guide*: Provides installation and upgrade procedures as well as tips for optimizing the performance of the Sun ONE Directory Server
- *Sun ONE Directory Server 5.2 Administration Guide*: Provides the procedures for using the console and command-line tools to manage directory contents and configure the features of the Sun ONE Directory Server
- *Sun ONE Directory Server 5.2 Reference Manual*: Details the Sun ONE Directory Server configuration parameters, commands, files, error messages, and schema
- *Sun ONE Directory Server 5.2 Plug-In API Programming Guide*: Describes how to develop Sun ONE Directory Server plug-ins
- *Sun ONE Directory Server 5.2 Plug-In API Reference*: Details the data structures and functions of the Sun ONE Directory Server plug-in API
- *Sun ONE Server Console 5.2 Server Management Guide*: Discusses how to manage servers using the Administration Server and Java™ technology-based console
- *Sun ONE Directory Server Resource Kit 5.2 Tools Reference*: Describes how to install and use the Sun ONE Directory Server Resource Kit

You can now become a Sun ONE Directory Server Certified Engineer by going through Sun's certification program. For information about this professional development opportunity, go to [training.sun.com/US/certification/middleware/dir\\_server.html](http://training.sun.com/US/certification/middleware/dir_server.html).

Other useful information can be found at the following Web sites:

- Sun Support Services: [sun.com/service/support](http://sun.com/service/support)
- Training: [suned.sun.com](http://suned.sun.com)
- Sun ONE Services: [sun.com/service/sunps/sunone](http://sun.com/service/sunps/sunone)

**SUN™** Copyright 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054 U.S.A. All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

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 other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, Java, Solaris, and Sun StorEdge are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

RESTRICTED RIGHTS: Use, duplication, or disclosure by the U.S. Government is subject to restrictions of FAR 52.227-14(g)(2)(6/87) and FAR 52.227-19(6/87), or DFAR 252.227-7015(b)(6/95) and DFAR 227.7202-3(a).

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.

**SUN™** Copyright 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, Californie 95054 Etats-Unis. Tous droits réservés.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, Java, Solaris, et Sun StorEdge sont des marques de fabrique ou des marques déposées, ou marques de service, de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

CETTE PUBLICATION EST FOURNIE "EN L'ETAT" ET AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, N'EST ACCORDEE, Y COMPRIS DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DE LA PUBLICATION A REpondre A UNE UTILISATION PARTICULIERE, OU LE FAIT QU'ELLE NE SOIT PAS CONTREFAISANTE DE PRODUIT DE TIERS. CE DENI DE GARANTIE NE S'APPLIQUERAIT PAS, DANS LA MESURE OU IL SERAIT TENU JURIDIQUEMENT NUL ET NON AVENU.



Please  
Recycle



Adobe PostScript

**Learn More**

Get the inside story on the trends and technologies shaping the future of computing by signing up for the Sun Inner Circle program. You'll receive a monthly newsletter packed with information on the latest innovations, plus access to a wealth of resources. Register today to join the Sun Inner Circle Program at [sun.com/joinic](http://sun.com/joinic).

To receive additional information on Sun software, products, programs, and solutions, visit [sun.com/software](http://sun.com/software).

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA Phone 800 786-7638 or +1 512 434-1577 Web [sun.com](http://sun.com)



**Sun Worldwide Sales Offices:** Africa (North, West and Central) +33-13-067-4680, Argentina +5411-4317-5600, Australia +61-2-9844-5000, Austria +43-1-60563-0, Belgium +32-2-704-8000, Brazil +55-11-5187-2100, Canada +905-477-6745, Chile +56-2-3724500, Colombia +571-629-2323, Commonwealth of Independent States +7-502-935-8411, Czech Republic +420-2-3300-9311, Denmark +45 4556 5000, Egypt +202-570-9442, Estonia +372-6-308-900, Finland +358-9-525-561, France +33-134-03-00-00, Germany +49-89-46008-0, Greece +30-1-618-8111, Hungary +36-1-489-8900, Iceland +354-563-3010, India-Bangalore +91-80-2298989/2295454; New Delhi +91-11-6106000; Mumbai +91-22-697-8111, Ireland +353-1-8055-666, Israel +972-9-9710500, Italy +39-02-641511, Japan +81-3-5717-5000, Kazakhstan +7-3272-466774, Korea +822-2193-5114, Latvia +371-750-3700, Lithuania +370-729-8468, Luxembourg +352-49 11 33 1, Malaysia +603-21161888, Mexico +52-5-258-6100, The Netherlands +00-31-33-45-15-000, New Zealand-Auckland +64-9-976-6800; Wellington +64-4-462-0780, Norway +47 23 36 96 00, People's Republic of China-Beijing +86-10-6803-5588; Chengdu +86-28-619-9333; Guangzhou +86-20-8755-5900; Shanghai +86-21-6466-1228; Hong Kong +852-2202-6688, Poland +48-22-8747800, Portugal +351-21-4134000, Russia +7-502-935-8411, Singapore +65-6438-1888, Slovak Republic +421-2-4342-9485, South Africa +27 11 256-6300, Spain +34-91-596-9900, Sweden +46-8-631-10-00, Switzerland-German 41-1-908-90-00; French 41-22-999-0444, Taiwan +886-2-8732-9933, Thailand +662-344-6888, Turkey +90-212-335-22-00, United Arab Emirates +9714-3366333, United Kingdom +44-1-276-20444, United States +1-800-555-9SUN or +1-650-960-1300, Venezuela +58-2-905-3800