

# SOLARIS™ NAMING AND DIRECTORY SERVICE

## THE SOLARIS™ OPERATING ENVIRONMENT

The Solaris™ 8 Operating Environment is the established OS leader for availability, scalability, and security in the Internet age. In Solaris 8 software, Sun delivers a trustworthy, universal platform to meet the needs of .com businesses — from small startups to large Fortune 1000 enterprises.

It's no surprise that the Solaris Operating Environment is the leading UNIX® environment today. Solaris software was originally designed with the Internet in mind. TCP/IP, the central Internet protocol, has been at the core of Solaris networking for more than 15 years. Through its time-tested design — a small, stable kernel, modular and extensible components, and well-defined interfaces — Solaris software delivers rock-solid stability and predictability for business-critical applications. And the Solaris 8 Operating Environment provides complete compatibility with prior versions, so you can be confident that your current applications will continue to run.

## SOLARIS NAMING AND DIRECTORY SERVICE

Solaris Naming and Directory Service combines standard naming and directory technology with enhanced security to provide a comprehensive and reliable naming service. Solaris 8 introduces the Lightweight Directory Access Protocol (LDAP) as an access protocol for naming services. LDAP is a simple protocol, but delivers a fairly robust set of features capable of supporting a diverse set of applications. Apart from update and access capabilities, LDAP also offers a rich set of features for searching. In addition to LDAP support, Solaris software continues to support the Domain Name System (DNS), Network Information Service (NIS), and NIS+ protocols. This provides businesses with a variety of choices in the area of naming and directory services when planning computer networks.

## LDAP AS A NAMING SERVICE

Solaris 8 introduces support for LDAP as the access protocol for naming services. LDAP is a directory standard defined by the Internet Engineering Task Force (IETF). The Solaris 8 Operating Environment lets you define information such as usernames, host names, passwords, and other network resources on any directory server (for example, the iPlanet™ Directory Server) supporting the LDAP v3 protocol. The LDAP server stores this information in a hierarchical namespace called a Directory Information Tree (DIT). The DIT consists of entries that are composed of attribute-value pairs. Each attribute has a type and can have one or more values. Naming information, such as host names and passwords, will be stored in these entries as attribute values.

In the Solaris 8 Operating Environment, LDAP clients can use the LDAP v3 protocol to access naming information from LDAP servers. The LDAP server must support the object classes and attributes that map the Network Information Service model onto LDAP. Several schemas related to Solaris processes, extended accounting, and more are also supported.

Solaris clients can currently authenticate to the LDAP server using anonymous and simple mechanism. LDAP can also support authentication using CRAM-MD5 if the server supports it. Additional protection is provided through access control, allowing the server to grant access for certain containers and/or entries. Access control is specified in the form of access control information (ACIs) on the server. Access rights for the directory objects can be specified as read and write, with these rights determining what the clients can do to or with the objects. Clients may be users or applications.

- Introduces LDAP as a naming service
- Offers a choice of naming service protocols: LDAP, DNS, NIS, and NIS+
- Provides support for NIS schemas in LDAP naming service
- NIS+ and LDAP support:
  - Hierarchical namespaces for ease in manageability
  - Incremental updates to the namespace
  - Multiple domains in a single namespace
  - Authentication
- LDAP supports ACI for users or applications
- Support for the DNS BIND 8.1.2 implementation

## **SUPPORT FOR DNS BIND 8.1.2**

The Solaris 8 Operating Environment supports the BIND 8.1.2 implementation of DNS. DNS is the standard method for mapping Internet domain names to IP addresses. BIND 8.1.2 supports improved performance over thousands of zones, providing the ability to consolidate the number of DNS servers deployed across the network.

### **BIND 8.1.2 SUPPORTS**

- DNS Dynamic Updates (RFC 2136)
- DNS Change Notification (RFC 1996)
- Flexible categorized logging system
- IP address-based access control for queries and zone transfers

## **ENHANCE SECURITY AND FLEXIBILITY WITH NIS+**

While DNS focuses on making communication simpler by using machine names instead of numerical IP addresses, NIS+ focuses on making network administration more manageable by providing centralized control over a variety of network resources. NIS+ stores information not only about machine names and addresses, but also about users, network services, and the network itself. This collection of network information is referred to as the NIS+ namespace.

NIS+ is a powerful network information service that supports secure access to network information with support for very large hierarchical namespaces independent of the transport-protocol and media deployed. It extends and improves the capabilities of NIS and DNS by implementing powerful authorization and authentication methods to increase security over the use of network resources. Additionally, it allows for the creation of multiple domains in a single namespace.

The security system implemented in NIS+ allows control over a particular user's access to individual entries in a specific table. This approach to security helps to keep the system secure as well as enabling administration tasks to be more broadly distributed without risking damage to the entire NIS+ namespace or even to an entire table.

## **CONTINUED SUPPORT FOR NIS**

NIS is a widely deployed and reliable distributed naming service. It uses a distributed database to identify and locate network objects and resources, and provides a uniform storage and retrieval method for network-wide information over TCP/UDP protocols.

By running NIS, system administrators can distribute administrative databases, called maps, among a variety of servers and update these databases from a centralized location in an automatic and reliable fashion. This ensures that all clients share the same name service information in a consistent manner throughout the network.

## **FUTURE DEVELOPMENTS IN NAMING AND DIRECTORY SERVICES**

In keeping with Solaris software's position as the market leader in Internet operating environments, Sun is committed to enhancing Solaris Naming and Directory Service functionality. Future plans will include:

- **Security:** The Solaris Naming and Directory Service will incorporate security for authentication, data integrity, and confidentiality
- **Interoperability:** Sun is committed to the LDAP standard, and will provide Solaris software with the ability to enable applications to use LDAP as a naming service
- **Continued support for the BIND implementation of DNS**

## **FOR MORE INFORMATION**

To learn more about Solaris Naming and Directory Service and the Solaris Operating Environment, please visit our Web site at [www.sun.com/solaris/](http://www.sun.com/solaris/).