Secure WAN Boot — Toward a Lights-Out Environment

White Paper
February 2004

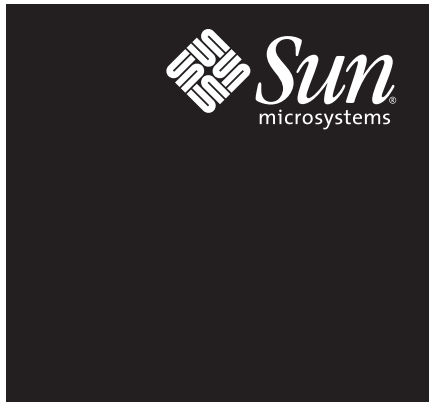


Table of Contents

Chapter 1

Introduction

Many customers would like to consolidate their installation and deployment operations to one central location, booting and installing software on servers deployed in lights-out facilities around the world. To help customers meet this goal, Sun has developed the Secure WAN Boot technology.

Secure WAN Boot technology provides a method to securely boot and install systems over the Internet with authentication of the client and secure transmission of the install image. This new technology, introduced in the Solaris™ 9 Operating System (OS), is the first of its type to be provided by a major UNIX® vendor. It helps IT departments manage a lights-out environment by enabling administrators to remotely install systems over geographically dispersed areas.

JumpStart™ software, Sun's current network install utility, works well on Local Area Networks (LANs), but is not a scalable option for customers who need to provision systems for remote sites. While the Solaris 8 OS provides the Dynamic Host Configuration Protocol (DHCP) as an option for network configuration during remote boot, the balance of JumpStart software's remote boot process relies on NFS version 2 or 3 for downloading the operating system and installation images. NFS lacks the security mechanisms required by Internet service providers (ISPs) and others who desire secure wide area network (WAN) installations.

A further issue with DHCP is that it is a LAN-based, rather than WAN-based, protocol that requires a DHCP server or relay server for every subnet. Using per-subnet DHCP servers creates a scalability bottleneck for customers with high numbers of installation sites and tight space requirements. In addition, NFS does not perform well in high-latency, low-bandwidth environments (WANs), and requires an NFS install server per site. Figure 1-1 illustrates the security and infrastructure issues associated with using the JumpStart software over a WAN.

© 2003 Sun Microsystems, Inc.

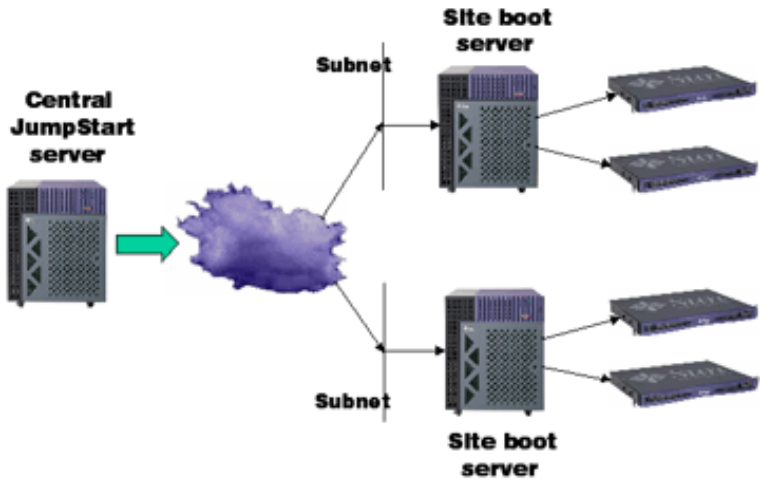


Figure 1-1: JumpStart software over a WAN is insecure and requires additional infrastructure

Secure WAN Boot technology uses a digital signature (SHA1) in the first stage of the boot process, then utilizes HTTPS (HyperText Transfer Protocol Secure sockets), Triple Data Encryption Standard (3DES), and Secure Hashing Algorithm 1 (SHA-1) (see Chapter 2) to solve most of the security issues that arise when using the JumpStart software to install systems over WANs. It also eliminates the need for per-subnet DHCP servers or relays and per-site NFS servers at the remote site, as shown in Figure 1-2.

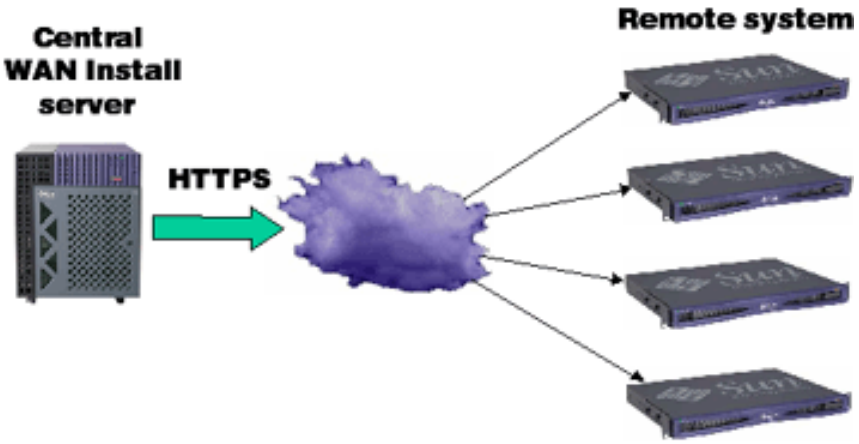


Figure 1-2: Secure WAN installation with Secure WAN Boot technology

Providing Security

Secure WAN Boot technology provides security over the Internet and insecure WANs with the following measures:

- Peer Authentication — It verifies the identities of the client and server by exchanging digital certificates (after the security payload has been downloaded, see Chapter 3).
- Data Confidentiality — It encrypts all of the information for transmission to prevent a third party from reading it.
- Data Integrity — It uses digital signatures and secure connections to verify that a third party has not modified the information received.

In addition, using a standard base configuration can help increase the security of individual systems by ensuring that unnecessary software is removed from all systems that provide specific functions. For example, a standard configuration for Web servers could be created that uses a stripped-down, secure version of the Solaris OS. Since every Web server uses the exact same configuration, and is essentially a clone of the original, the chances of a security breach due to a configuration error are significantly reduced.

Lowering TCO

Using Secure WAN Boot technology for Internet-based installs can help lower a company's total cost of ownership (TCO) by:

- Reducing necessary infrastructure (JumpStart servers, disk space) by using compressed Flash archives and eliminating per-subnet NFS servers
- Enabling secure system deployments over WANs both locally and remotely, decreasing the need for senior administrators at remote sites
- Reducing network costs by using public networks
- Increasing efficiency by centralizing administration: Difficult administration tasks (setting up install and boot servers) can be centralized; junior administrators can install remote systems per company standards in a consistent, secure manner
- Increasing scalability by enabling remote installations of additional systems
- Automating upgrades — Situations where initial installations are acceptable (Flash archives overwrite existing software)

Who Will Benefit

The security and increased speed features of the Secure WAN Boot technology will be beneficial in many environments, including:

- Data centers — Where security might not be as crucial, but TCO is
- E-commerce and (ISP) environments — Where scalability, flexibility, consistency, and security are paramount issues
- Trading floors and banks—Where increased security, consistency, central administration, efficiency, and reduced infrastructure have a tremendous impact on lowering TCO
- Government agencies and others providing services to remote locations — Where there is a need for centralizing administration, increasing security, and reducing or eliminating the cost of sending administrators to remote sites
- Any enterprise — With the need to install systems over a WAN in a consistent and secure manner in order to increase scalability, flexibility, and efficiency while decreasing administration and infrastructure costs

Secure WAN Boot support in the boot Programmable Read-Only Memory (PROM) is planned for the majority of new Sun platforms. Legacy UltraSPARC® systems are supported via a local copy of the `wanboot` executable, explained in Chapter 3. Secure WAN Boot servers must be running the Solaris 9 OS, while client installations are supported for the Solaris 8 OS (update 5) or later.

Secure WAN Boot technology is basically performed in two steps: 1) *Setting up the install and boot servers*, and 2) *Installing the remote client*. These steps are discussed in more detail in the following pages.

Chapter 2

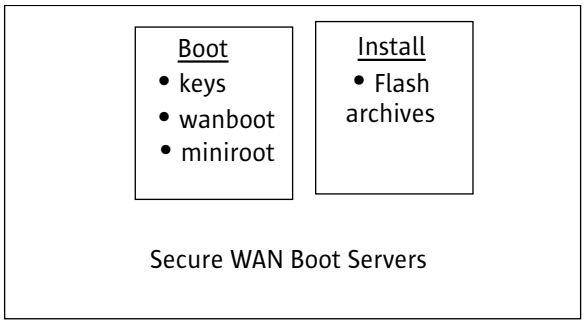
Setting Up the Install and Boot Servers

There are two distinct server functions required for the Secure WAN Boot technology as shown in Figure 2-1. They are:

- An install server, to provide install images
- A boot server, to provide second-stage boot (`wanboot`), third-stage boot (Solaris OS miniroot) images, and per-client security payloads

These functions, while individually contained, may be run on a single system or distributed across multiple systems. The initial set up of the install servers is required only once for an entire network. Install images can be added as needed, and additional servers can be employed to support large numbers of simultaneous client installations. In the future, a utility will be provided to automate the configuration of the required servers.

Figure 2-1: Secure WAN Boot servers and their contents



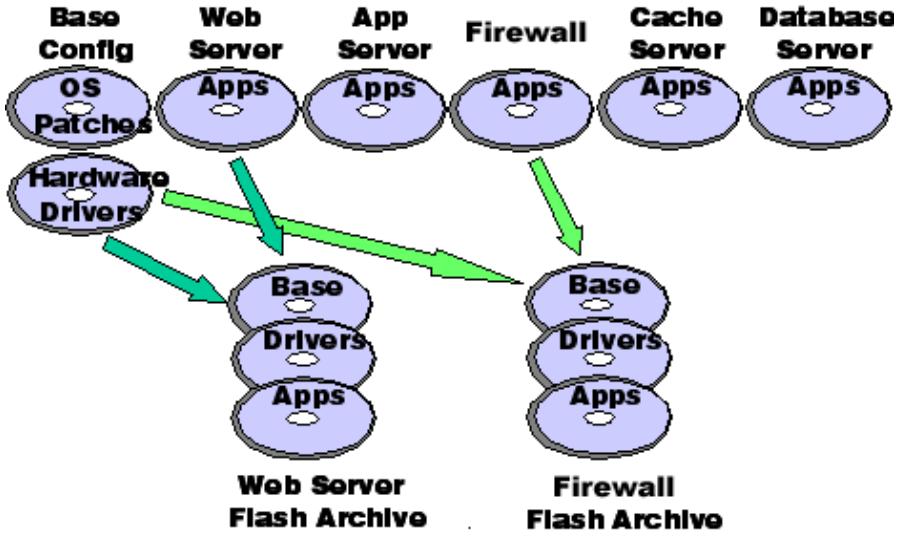
Setting Up the Install Image Server

The install server contains the Flash archives of the various client configurations available for Secure WAN Boot technology. Each install image archive should contain the base configuration, for example, the Solaris OS for the target platform and patches, as well as the appropriate hardware drivers and the application profile for the desired system service.

Creating and Testing a Configuration

A base configuration, containing the Solaris OS and current patches for the type of server to be installed, must be created and thoroughly tested. The administrator then determines which hardware will be resident on the target system and installs the corresponding drivers and any necessary patches. For a modular approach, application profiles can be created and added to the base configuration to create specific service images, for example, application server, database server, Web server, and cache server. Figure 2-2 shows how base configurations and application profiles can be combined to create service images and the resulting Flash archives.

Figure 2-2: Base configurations, application profiles, and Flash archives



 © 2003 Sun Microsystems, Inc.

Creating a Flash Archive

After a service configuration has been created and tested, a Flash archive can be created from it. The Flash technology enables administrators to create a snapshot image of a complete system, including the Solaris OS, applications, and system configuration. When a Flash archive is installed on a system, all of the files in the archive are copied to that system, giving the newly installed system the same installation configuration as the original system. Installing a new system with Flash archives is much faster than using a JumpStart software image since the files are simply copied to the target system, rather than installed individually through `pkgadd`. Once the archives have been created, they can be moved to the install server.

Setting Up the Boot Image Server

The boot image server provides the per-client security payloads, `wanboot` executable, Solaris OS miniroot, and appropriate utilities, libraries, and files to allow the Solaris OS miniroot to boot and run installation software on the client system. Detailed instructions for setting up all of the Secure WAN Boot servers can be found in *Secure WAN Install — Setting Up Install Servers*.

Creating the Shared Keys

For each client, it is necessary to configure the boot server with information to allow the client to be identified and authenticated. This includes placing a pair of keys onto the client system and boot server. This key pair — the “shared keys” — is normally unique for each client, but may be used on all clients depending on the level of security required.

The first key is an SHA-1 symmetric authentication key used for signing and authenticating the `wanboot` binary. The second is a 3DES symmetric encryption key used for encrypting and decrypting the security payload.

Secure WAN Boot technology provides utilities to help add new install clients, and tools that enables customers to implement or integrate with an appropriate configuration and key management infrastructure.

Note – The shared secret keys are resident on the client in the boot PROM, and can be accessed by any application that can access the boot PROM `nvram` (should only be accessible by `root`) or from the console (which should be physically secure).

Chapter 3

Installing the Client System

Installing a Secure WAN Boot client system consists of three main stages:

- Booting the remote client and downloading the `wanboot` binary
- Executing the `wanboot` binary and downloading the WAN Boot security payload and Solaris OS miniroot
- Executing the miniroot, which downloads and installs the install image

Booting the Remote Client

During the initial boot process, the remote system local interface is configured (for example, remote system IP address, remote system host name, and so on) and the address of the boot server is specified. If they are not already present, the shared keys should be set. The remote system then downloads the `wanboot` executable from the boot server. These steps are discussed in more detail below.

Initial Boot

Normally, a client has a secure console connection that is used to initiate the installation. Alternatively, the system can be configured to automatically install software when it is powered on (a console connection is needed to deal with any errors).

Prior to starting the `wanboot` download, the remote client network interface must be configured; the following parameters must be set:

- Client IP address
- Client host name

 © 2003 Sun Microsystems, Inc.

- Client subnet mask
- Client default router IP address

Additionally, the boot server address must be specified.

These parameters may be specified from the Open Boot Prom (OBP) command line by setting the OBP environment variable, `network-boot-arguments`:

```
ok setenv network-boot-arguments host-ip=<IP address>,...
```

or they may be specified as additional arguments to the `'boot net'` command (see below).

It is possible to use DHCP to supply the parameter values by setting `network-boot-arguments` to `'dhcp'`:

```
ok setenv network-boot-arguments dhcp
```

or by using an alternative form of the `'boot net'` command (see below).

If the shared keys are not already present on the client, they should be specified using the OBP command:

```
ok set-security-key <keyname=keyvalue>
```

The OBP command used to download the `wanboot` binary is:

```
ok boot net <optional arguments> - install
```

or, to use DHCP to provide the client interface configuration:

```
ok boot net:dhcp <optional arguments> - install
```

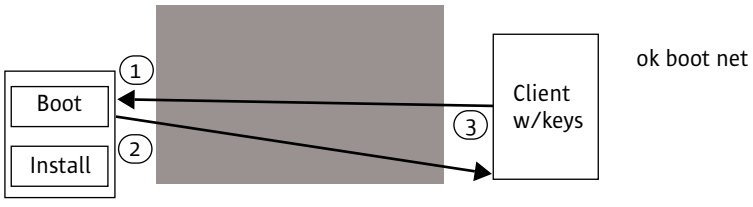
The boot PROM downloads the second stage boot (`wanboot` executable), which is accompanied by a digital signature signed with the server's copy of the shared authentication key. The OBP will only execute a correctly signed `wanboot` binary. Figure 3-1 illustrates the downloading process.

For systems without Secure WAN Boot support in the boot PROM, the `wanboot` can be performed by executing the `wanboot` binary provided on the install media; for example:

```
ok boot cdrom -F wanboot -o prompt - install
```

Note the use of the `'-o prompt'` argument; this causes `wanboot` to prompt for the necessary interface configuration parameters, boot server address, and shared keys.

Figure 3-1: Boot and download process



Executing the Wanboot Binary

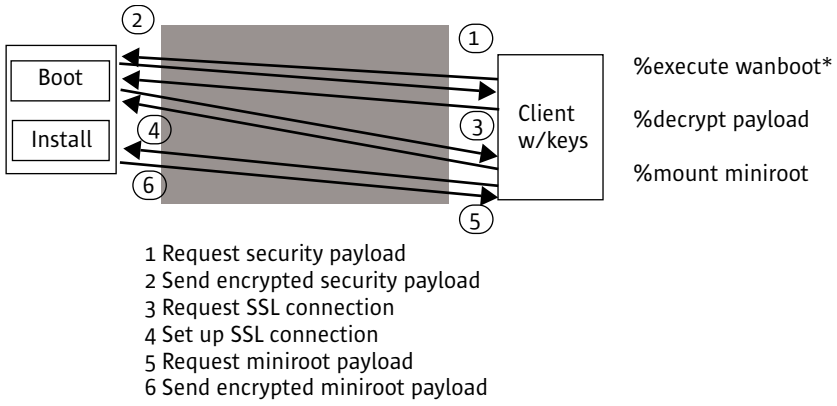
The OBP executes the `wanboot` binary, which then downloads a security payload that has been signed with the client's authentication key and encrypted with the client's encryption key from the install server. The security payload contains the message digest algorithm type, the client's private key, and the client certificate. The certificate authority (CA) certificate is downloaded within the security payload and is used to set up the Secure Sockets Layer (SSL) connection. It is the means by which SSL authenticates the boot/install server. The client certificate and private key are used by SSL to authenticate the client.

After the payload is decrypted, `wanboot` uses the certificate and client key to authenticate identities and set up a secure SSL connection between the client and the install server. (Secure WAN Boot technology supports a subset of the standard SSL encryption algorithms.) The administrator has the option to disable SSL if a secure HyperText Transfer Protocol (HTTP) transaction is not needed, for example, on secure private networks.

Next, `wanboot` uses this authenticated, encrypted connection to download a boot file system image that contains a copy of the Solaris OS miniroot and the appropriate utilities, libraries, and files to allow the Solaris OS miniroot to boot and run the installation software (Figure 3-2). Using an encrypted connection helps ensure confidentiality of the transmitted data.

If the boot file system is valid, `wanboot` mounts it and the Solaris OS miniroot is extracted. The miniroot is then executed.

Figure 3-2: SSL connection and download process

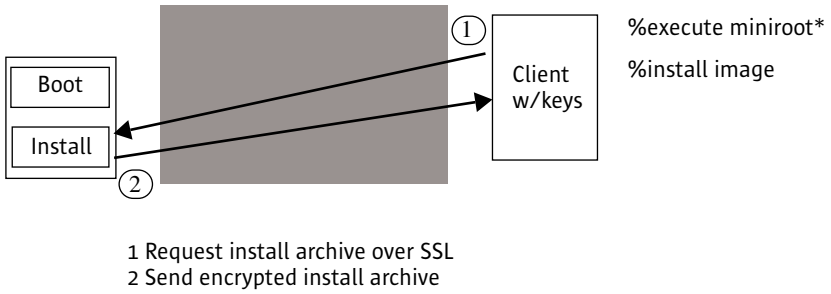


*Not actual commands, for illustration only

Executing the Miniroot and Installing

When the Solaris OS miniroot executes, it starts the install process which retrieves the SSL certificates used by `wanboot` (passed to the client in the security payload) and uses them to enable a secure download of the Flash archive image from the install server, as depicted in Figure 3-3.

© 2003 Sun Microsystems, Inc.



1 Request install archive over SSL
2 Send encrypted install archive

*Not actual commands, for illustration only

Figure 3-3: Miniroot execution, download, and install process

Summary

Considering the economic uncertainty of the times, the need to cut costs and increase productivity is at the forefront of every IT manager's mind. Secure WAN Boot technology helps address these needs by giving administrators the ability to install systems over the Internet in a secure and efficient manner. With products like Secure WAN Boot technology, Sun is helping companies cut costs and enabling them to move one step closer to a lights-out environment.

Chapter 4

References

Sun Microsystems posts complete information on its hardware and software products and service offerings in the form of data sheets, specifications, and white papers at sun.com.

- Sun BluePrints™ papers:
  - *Building a Bootable JumpStart Installation CD-ROM* by John S. Howard
  - *WebStart Flash* by John S. Howard and Alex Noordergraaf

- Other:
  - *Web Security, Privacy & Commerce* by Simson Garfinkel, O'Reilly Publishers

Chapter 5

Glossary

- **Cryptography**: Mathematical techniques for protecting information.
- **3DES**: Triple Data Encryption Standard: A block encryption algorithm, encrypting data blocks of 64 bits at a time with 56-bit keys (original DES) or 112-bit keys (3DES).
- **Digital certificates**: A general-purpose identification system that uses public key cryptography. It is a signed block of data that contains a public key and other information, such as a person's name and e-mail address.
- **Message digest**: Message digest functions distill the information contained in a file into a single large number, usually between 128 and 256 bits in length. They are sometimes referred to as "one-way hash" functions because they produce values that are difficult to invert, resistant to attack, effectively unique, and widely distributed. Message digest algorithms are used to create digital signatures, message authentication codes, and encryption keys.
- **SHA-1**: A revised version of the Secure Hashing Algorithm designed for use with the National Institute for Standards and Technology's Digital Signature Standard.
- **SSL**: Secure Sockets Layer: A general-purpose Web cryptographic protocol for securing bidirectional communication channels.
- **Symmetric authenticating key**: The same key is used for encrypting and decrypting.

Note – Definitions are from *Web Security, Privacy & Commerce* by Simson Garfinkel, O'Reilly Publishers

---

SUN™ Copyright 2004 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, JumpStart, Solaris, and Sun Blueprints 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 2004 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, JumpStart, Solaris, et Sun Blueprints 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.

To receive additional information on Sun software, products, programs, and solutions, visit 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

Sun microsystems
We make the net work.

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 +421-2-4342-94-85, 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 02/04 R1.0