SUN BLUEPRINTS APPROVED

Using pGINA to Authenticate Users in Microsoft Windows Environments

Dave Pickens, Research and Academic Computing

Kent Price, Research and Academic Computing

Sun BluePrints™ OnLine—June 2004

`http://www.sun.com/blueprints`

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95045 U.S.A.
650 960-1300

Part No. 817-7043-10
Revision 1.0, 6/9/04
Edition: June 2004

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.

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.

Using pGINA to Authenticate Users in Microsoft Windows Environments

This article describes the use of pGINA, which simplifies the authentication of Microsoft Windows users in an environment that includes Window, Linux, and UNIX® systems. The objectives of this article are to provide you with a basic understanding of how authentication in a Windows environment works, and how pGINA can be used to provide an alternative authentication mechanism in a heterogeneous environment. This article provides recommendations for when pGINA should be used, and when it might not be a good idea to use.

This article is intended for technical people who are interested in directory services and the integration of Microsoft Windows into a heterogeneous environment.

The following sections define the problem, offer a solution to the problem, and provide a case study as an example of a successful deployment of the solution:

- "The Problem" on page 2
- "The Solution" on page 5
- "VCSU – A Case Study" on page 10

The Problem

There are a number of problems to consider when setting up a unified authentication scheme in a UNIX-based computing environment that includes Microsoft Windows.

1. Windows simply doesn't play nice. When authentication is used in a Windows environment, Windows, by default, wants to use its own authentication mechanism and it doesn't provide the ability to easily use other authentication mechanisms. Because Windows makes it difficult to use other authentication mechanisms, users often don't make an effort to use a method that might be more secure and make overall administration easier.

2. Windows support is another problem. Support for 95/98/Me is ending. Support for Windows 95 ended in 2000 and paid extended support ended in 2001. Windows 98 support ended in 2002 with paid extended support ending in 2006, and Windows Me support ended in 2003 with paid extended support until 2006.

3. Microsoft has also announced that they will stop supporting Windows NT. Security and hot fix support for Windows NT is available through 2004. Any other support is available only with a custom support contract.

4. For a number of reasons, not the least of which is price and Microsoft's licensing policies, many institutions are now looking to utilize other operating systems in the data center. Many institutions are moving to UNIX/Linux.

All of these issues pose problems for system administrator's ability to have a single unified authentication mechanism.

Typical Authentication Architecture

Typically, data centers implement Windows using the default Windows authentication services. This means they implement either a standalone authentication architecture or they implement one based upon Active Directory. If they have a heterogeneous environment and have UNIX servers as well as Windows servers, they may end up with two entirely separate authentication mechanisms—one for UNIX and one for Windows (FIGURE 1). This presents problems for administration because two separate services must be maintained. Therefore, when a user needs to be added, the administrator must add the user in both directories.

At best, they will set up both an LDAP directory for UNIX and an Active Directory server for Windows, and then use some form of synchronization software between the two (for example, Sun Java™ System Identity Synchronization for Windows). This solves some of the problems, but there are still two authentication services as well as an additional component that must be maintained.

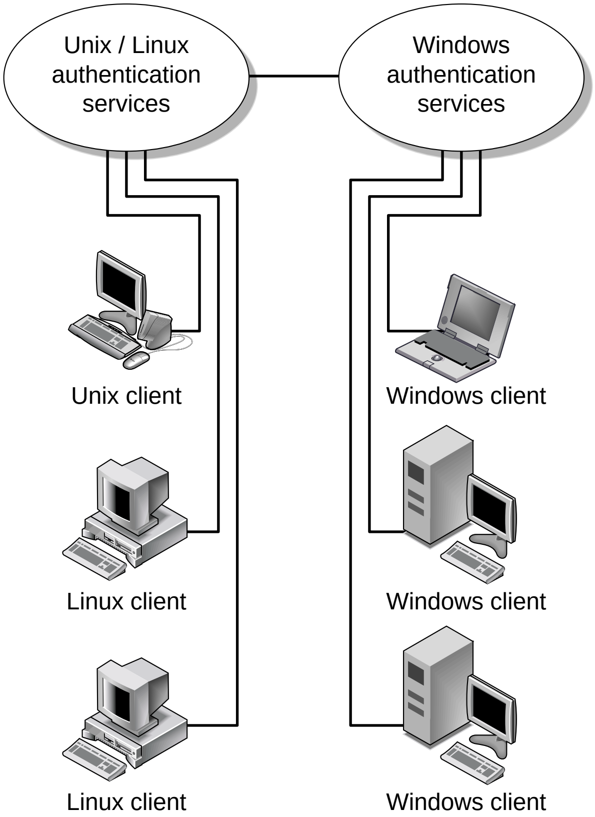


FIGURE 1 Typical Authentication Architecture

Ideal Authentication Architecture

The ideal authentication architecture is to maintain a single authentication directory and have both UNIX and Windows clients authenticate to it.

This is where Windows starts to fall down: the standard Windows Authentication mechanism doesn't allow for this.

Using the ideal authentication architecture (FIGURE 2), UNIX and Windows clients talk directly to the UNIX authentication service, bypassing the use of Active Directory. But how do you get there?

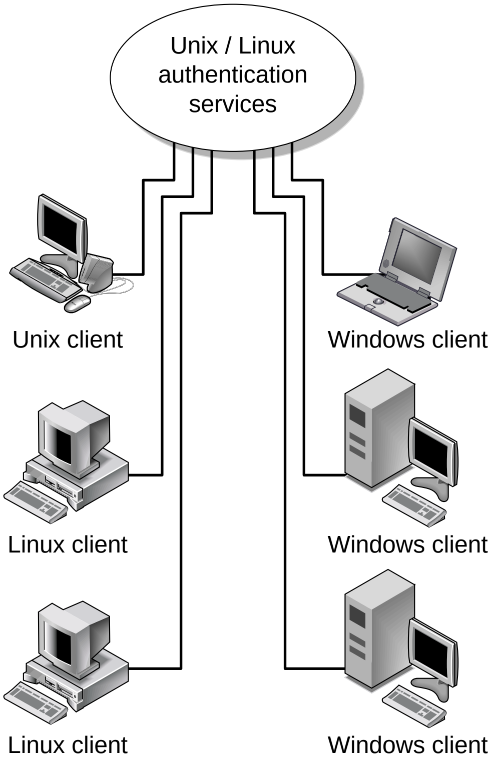


FIGURE 2 Ideal Authentication Solution

The Solution

The answer to this problem is to use pGINA.

Before we talk about pGINA, let's talk specifically about how things work. Windows by default, uses something called GINA for authentication.

What is GINA?

GINA stands for Graphical Identification and Authentication. GINA is a dynamic-link library (DDL) that is part of the Windows operating system. GINA is loaded early in the boot process by `Winlogon.exe`. Once loaded, GINA handles the following functions:

- SAS Recognition – Stands for secure attention sequence recognition. The GINA can have its own SAS, and carries the responsibility of recognizing the SAS. This is not required if the GINA decides to use the Standard SAS of the `WinLogon.exe` (Ctrl + Alt + Del). The GINA makes the appropriate calls, depending on the current state of the station. If the GINA uses the standard SAS, the `WinLogon.exe` automatically calls the appropriate routine.
- User Interface – Since the GINA can provide an alternative identification mechanism, it is the responsibility of GINA to display the entire user interface that is needed to perform the logon authentication. The GINA has to display the user interface to collect data needed to perform the authentication, and all other user interfaces depending on the state of the station.
- Shell Creation – When a user performs a successful logon, the GINA works with `WinLogon.exe` to create the initial processes and assign the processes that the user's access token obtained from the `WinLogon.exe`. This process must start the default shell for the user. Normally, `userinit.exe` is started as the initial process. This program is run in the user’s context and the user’s desktop. It sets up the user environment by restoring the network connection, loading the user’s profile (color, font, screen savers, and so on) and running logon scripts. It then activates the shell programs with the same environment as itself. The standard shell for Windows NT is `Explorer.exe`. This program manages the desktop, taskbar, and so on. Once the shell is created with the user’s access token, all other processes created by the user automatically inherit it, thus securing the resources.

Windows Authentication Architecture

During a power-on or boot-up sequence (FIGURE 3), the `Winlogon.exe` process is started. This process continues to run in the background during the entire time the OS is loaded.

When a user issues the SAS to logon, the `Winlogon.exe` process calls the GINA DLL to handle the user identification and authorization process. GINA presents a logon dialog for the user to fill out. Using this dialog, GINA acquires the information it needs to authenticate the user.

GINA then contacts either the Active Directory or the Domain Controller. After GINA has validated the user, it returns a token and control to the `Winlogon.exe` process, which in turn starts a user-level shell using the permissions of the user and then creates the user's environment using the authenticated user’s environment settings and appropriate scripts.

Once the user's shell and environment is set up, `Winlogon.exe` turns control of the shell over to the user.

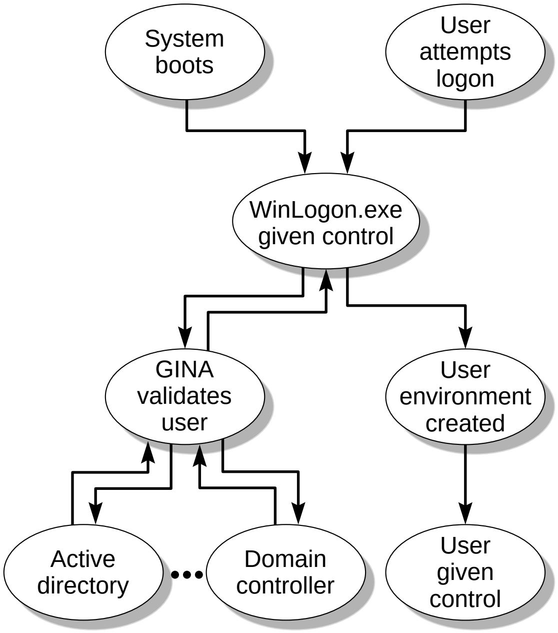


FIGURE 3 Windows Authentication Architecture

What is pGINA?

pGINA stands for Pluggable Graphical Identification and Authentication.

pGINA is an add-on DLL for the standard Microsoft GINA and provides a framework that allows different methods of authentication. These are implemented by the use of authentication plug-ins

Just as pluggable authentication module (PAM) technology brings different authentication methods to UNIX, pGINA brings this same functionality to the Windows environment.

pGINA provides the skeleton code necessary to quickly and easily implement many different methods of user authentication. Once a plug-in has been created for a particular authentication method, it can be easily installed on multiple systems. The new plug-in can be made available to other users without the users needing an in-depth understanding of the Windows logon process. Some of the plug-ins that already exist for pGINA are OpenLDAP and Radius. Available plug-ins are discussed later.

Windows Authentication Architecture With pGINA

When using pGINA, the process is the same as with GINA except the user issues a SAS to logon, the `WinLogon.exe` process calls the pGINA DLL to handle the user identification and authorization process. pGINA presents a logon dialog box for the user to fill out. Using this dialog box, pGINA acquires the information it needs to authenticate the user. pGINA passes any information or requests that it is not configured to handle to the GINA DLL for processing.

Depending on the configuration, pGINA then authenticates the user by using whichever authentication modules are needed. If pGINA is configured to use LDAP, pGINA uses the LDAP plug-in that authenticates through LDAP on behalf of the user—typically called a *bind* or referred to as *binding* to the directory. pGINA can also be configured to chain the authentication methods so that multiple methods are used. This is represented as by ellipsis in FIGURE 3.

Once pGINA has validated the user, it passes any configuration information and returns a token and control to the `WinLogon.exe` process (FIGURE 4). This, in turn, starts a user-level shell with the permissions of the user logging in and then creates the user's environment by using the authenticated users environment settings and appropriate scripts, and so on. Once the user's shell and environment is set up, `WinLogon.exe` turns control of the shell over to the user.

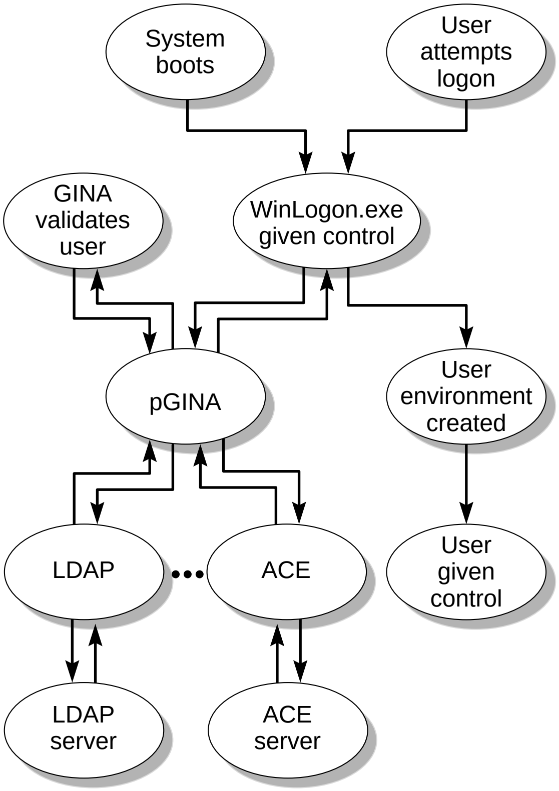


FIGURE 4 Windows Authentication Architecture With pGINA

Available Plug-ins

There are currently a total of nine publicly available plug-ins from `http://pgina.xpasystems.com`[1]:

LDAPAuth – For authentication against an LDAP server

Chaining Plug-in – Allows you to *stack* individual plug-ins

PAM for pGINA – For authentication with UNIX PAM

MySQLAuth Plug-in – For authentication against a MySQL database

POP3 Plug-in – For authentication against a POP3 mail server

NIS Plug-in – For authentication against an NIS server

[1] List of plug-ins obtained from the XPA Systems web site for pGINA.

ACE (SecureID) Plug-in – For authentication to a domain with RSA's SecureID product

OpenAFS Plug-in – For authentication against an AFS realm

RADIUS Plug-in – For authentication and accounting with RADIUS

Good Situations for pGINA

There are several scenarios where pGINA is a good fit for a particular environment:

- When you already have, or are going to implement, a mixed UNIX/Linux/ Windows environment.
- If you have already installed Active Directory and are struggling with it; or if you are in the planning stages of an Active Directory implementation.
- If you are migrating away from Windows 95, Windows 98, or Windows Me to Windows XP or Windows Server 200X.
- If you understand and appreciate the value of maintaining a single point of authentication.

Not So Good Situations for pGINA

There are also several scenarios where the implementation of pGINA might do more harm than good:

- You have a Microsoft-only environment.
- You don’t want to use UNIX or Linux naming services.
- You need Active Directory services for advanced Microsoft services such as Exchange.
- You have an extremely large number of clients. While supporting a large number of clients with pGINA is not impossible, it requires more care in the implementation phase.

Things to Consider

Before installing and using pGINA, plan carefully. The following list describes some of the areas that you should take into account:

- Policies – Determine which authentication policies you want to implement.
- Features – What pGINA features do you plan to implement? Which plug-ins suit your needs?
- Options – There are a number of options you can choose to implement. Do you want to replace the logo and other options?

- Testing – Implement the plug-ins and features in a test environment before deploying to your production environment.
- Piloting – It is a good idea to run a pilot program for pGINA with a select group of users.
- Rollout – Finally, roll out the approved configuration. If necessary, roll it out in a phased manner.

VCSU – A Case Study

This section describes a case study of a customer that is using pGINA.

Valley City State University or VCSU, is a small liberal arts college in Valley City, North Dakota, just south of Fargo.

VCSU is known as a teacher's college—that is, they educate K-12 teachers and provide post-graduate education to teachers.

VCSU isn't very large, but they have an edge with technology. They were one of the first colleges in the country to provide laptops to students as part of tuition, even before Dartmouth and other prestigious schools. Currently, they are implementing 802.11g wireless access across 80% of their campus, providing 54 Mbps throughput. Additionally, VCSU has roughly 2300 10/100 Mbps switched Ethernet connections across campus.

VCSU has an enrollment of roughly 1100 students and a faculty and staff of about 400.

The IT staff supports approximately 1200 Windows-based PCs: 1100 laptops and 100 desktops. These can be broken down into four profiles: student laptops, faculty laptops, administration desktops, and lab (public) desktops. The IT group has a total of 16 people, including part time assistants, who are responsible for all aspects of computing at the University.

Challenges

About two years ago, VCSU was faced with major changes. Support was coming to an end for Windows 95/98/Me as well as Windows NT. They knew they needed to make a change soon. However, they weren't thrilled with Microsoft and wanted to avoid the migration to Active Directory.

VCSU was using Novell’s Netware for base services such as login and authentication for several NT domains. These servers also provided both file and print services.

To reduce the use of the servers and avoid more Windows NT boxes, VCSU started offloading the print services by migrating to network-based printers with built-in support for Windows clients (as well as other standards).

The ultimate goal was to limit Microsoft to the desktop and have a better operating system for the backend systems. They standardized using Solaris™ and Linux operating systems.

Eventually, after moving services off of Microsoft, VCSU reduced their total number of servers for the core functions, from 14 down to 8.

Solution

VCSU's software architecture now consists of the following Sun software:

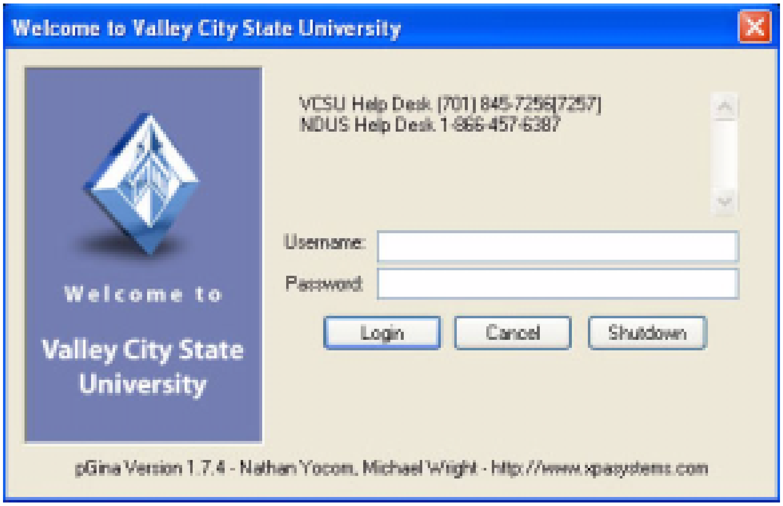
- LDAP by way of Sun directory server software using a multiple master configuration
- Email using the Sun messaging server software
- Campus-wide calendar services provided by Sun’s calendar server software
- A campus portal for learning using the Sun portal server software with single sign on (SSO) to their Blackboard Learning Management System (LMS)

Additional Software for a Complete Solution

The Sun products alone were not enough to provide the total solution. Other products were required to provide file services, desktop management services, software license management, and some network management. The following sections describe what VSCU used to fill in the gaps.

pGINA

pGINA provides the ultimate solution in regards to limiting Microsoft to the desktop. VCSU uses pGINA to avoid using Microsoft Active Directory by authenticating users to a Sun directory server. pGINA also affords VCSU the ability to customize the user login experience (FIGURE 5) and gives them more control over the desktop.



VCSU Help Desk [701] 845-7256[7257]
NDUS Help Desk 1-866-457-6387

pGina Version 1.7.4 - Nathan Yocom, Michael Wright - http://www.xpasystems.com

Welcome to Valley City State University
Welcome to
Valley City State University
Username:
Password:
Login
Cancel
Shutdown

FIGURE 5 Customized VCSU Login Window

SAMBA 2.2 for File Services Only (no print services)

Samba is configured to use Common Internet File System (CIFS) and normal Windows protocols with the clients while using LDAP with PAM on the Solaris server on the backend.

Norton Ghost for Desktop Management

Deploying updates as well as disk image management is key to keeping administration overhead low. VCSU has five or six standard disk images. Any additional software can be added by way of an authenticated web site. Desktops and laptops are reloaded each year at a minimum. Other Norton utilities are used for updates.

Sassafras for Software License Management

The additional software is centrally managed. VCSU chose Sassafras K2 as their license key software management product. This allows VCSU to deploy the software physically to many laptops, either as part of the default image or as an added option, while controlling licensing. For example, Adobe Photoshop is required for some class work but not all. Using Sassafras, VCSU only needs to purchase 150 licenses, yet Photoshop is loaded on all the laptops by default. When a user wants to use Photoshop, a license is checked out from the Sassafras server. Licenses are kind of like Dynamic Host Configuration Protocol (DHCP) addresses in that they are leased from the server for a period of time.

One interesting feature provided by the Sassafras software is the ability to set policies so that professors on campus get longer leases, say a week, compared with students who might only get a 24-hour lease. Microsoft Project is an application that is used from time-to-time by students and staff, but not routinely. It's not part of the standard image. When individuals on campus need to use the software, they log in to the Sassafras server and perform a network install. They obtain an initial license key in the same manner as described in the Photoshop example.

At any given time, the IT department can use the Sassafras management reports feature to see how many licenses are active versus how many total licenses are owned. At the end of the year, they can use these reports to make critical decisions about ongoing support and upgrade expenditures.

MRTG, Netflow Data, and Packeteer Packetshaper for Network Traffic Management

Multi Router Traffic Grapher (MRTG) is a graphical charting and reporting tool to monitor the traffic load on network links. It is used to monitor dozens of devices including routers, switches, firewalls, servers, modems, and UPSs. Netflow data is collected from the core router and processed to provide analysis of Internet Protocol (IP) flows. VCSU uses it to detect Denial of Service attacks, infected hosts, and peer-to-peer applications like Kazaa. Packeteer Packetshaper is an application traffic management appliance that provides bandwidth management control.

Cisco Pix for Firewalls

Cisco Pix security appliances provide the campus with the needed levels of network security.

Cisco Content Switch for Load Balancing

The new Cisco Content Switch is an updated version of the older Cisco Director product. It provides load balancing in a more *protocol aware* manner (for example, balancing takes place in higher layers of the OSI stack).

NetReg

NetReg is an automated system that requires campus users to register their hardware (MAC addresses) before gaining full network access in a DHCP environment. An LDAP module is used to authenticate the campus user during the registration process. It was developed by Southwestern University and is available under GNU license.

Supporting Hardware

Most of VCSU’s servers are Sun Fire™ 280R servers using Sun StorEdge™ A1000 devices for locally attached storage. The exceptions to this are at the lower level where services such as DHCP are delivered. In these cases, Sun Fire V120s and Sun™ LX50s servers are used.

More pGINA Success Stories

The following academic institutions are also taking advantage of the benefits of pGINA:

- Miami University – Ohio
- Curtin University of Technology – Australia
- University of Guelph – Canada
- Pacific Lutheran University – Washington
- University of Technology Sydney – Australia
- University of Calgary – Canada
- University of Malaga – Spain
- University of Sussex – England

Additional Information

You can obtain additional information about the topics in this article from the following URLs and publications:

XPA Systems web site for pGINA support: `http://pgina.xpasystems.com`

Valley City State University web site: `http://www.vcsu.edu`

Norton/Symantec web site: `http://www.norton.com`

Sassafras Software web site: `http://www.sassafras.com`

Fass, Ryan, “Short take: Using pGina to integrate PCs into a Mac server world”, ComputerWorld: September 10, 2003.

Yocom, Nathan, “PAM-like Authentication for Windows Clients”, Sys Admin Magazine: November 2002.

Miami of Ohio School of Engineering IT Group, `http://www.sas.muohio.edu/computing/pgina.html`

Sun BluePrints publications, `http://www.sun.com/solutions/blueprints/online.html`

Sun software products web site: `http://wwws.sun.com/software/`

Note – Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites. Sun will not be responsible or liable for any actual or alleged damage or loss caused by or in connection with the use of or reliance on any such content, goods, or services that re available on or through such sites.

About the Authors

Dave Pickens is an Enterprise Architect in the Academic and Research Computing Group at Sun Microsystems. He has over ten years experience in systems engineering, including large systems deployments such as SAP and PeopleSoft. His previous publications include a Sun Blueprints book titled *Sun ONE Messaging Server Practices and Techniques for Enterprise Customers*, and several articles on network diagramming tools for InfoWorld. Currently he is working on various projects with Sun's education customers involving the Java Enterprise System software products such as the directory server, messaging server, and the calendar server.

Kent Price is a systems engineer in the Academic and Research Computing Group at Sun Microsystems. He has over twenty years experience working in IT, including stints working as both a network and a UNIX administrator. His customers include Indiana University, Purdue University, and the University of Notre Dame. Kent's current projects include High Performance Computing clusters at Purdue and Notre Dame.

Ordering Sun Documents

The SunDocs^{SM} program provides more than 250 manuals from Sun Microsystems, Inc. If you live in the United States, Canada, Europe, or Japan, you can purchase documentation sets or individual manuals through this program.

Accessing Sun Documentation Online

The `docs.sun.com` web site enables you to access Sun technical documentation online. You can browse the `docs.sun.com` archive or search for a specific book title or subject. The URL is `http://docs.sun.com/`

To reference Sun BluePrints OnLine articles, visit the Sun BluePrints OnLine Web site at: `http://www.sun.com/blueprints/online.html`