IBM

Open Your Windows with Samba on Linux

- Linux requires fewer critical security updates
- Describes the just released Samba-3 with enhanced features
- Linux can lower your total cost of ownership

Stephen Hochstetler
Omkhar Arasaratnam
Rodrigo Castello Branco

Redpaper

ibm.com/redbooks

International Technical Support Organization

Open Your Windows with Samba on Linux

December 2003

Note: Before using this information and the product it supports, read the information in “Notices” on page v.

First Edition (December 2003)

This edition applies to Samba Version 3 with Red Hat Enterprise Linux ES Version 3, SUSE Linux Enterprise Server 8, and Turbolinux Enterprise Server 8.

Contents

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:
This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

AIX®	IBM®	Tivoli®
DFS™	ibm.com®	xSeries®
Domino®	Lotus®	zSeries®
@server™	Redbooks™	
eServer™	Redbooks(logo) ™	

The following terms are trademarks of other companies:

Intel, Intel Inside (logos), MMX, and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Forward

Over the last few years, Samba has begun to play an increasingly important role in allowing enterprises to bridge the gap between the worlds of Windows computing and traditional UNIX systems. One of the things that has slowed things down to some extent within IBM is the lack of a good set of supporting documentation in the form of Redbooks and Redpapers. I am delighted to see that this is now beginning to be addressed, and I hope that this Redpaper will be one of many that will help IBM take full advantage of Samba.

Andrew Tridgell
President, the Samba team

Preface

This paper addresses strategies for a migration from Microsoft® Windows® file and print servers to Samba on Linux file and print services. When migrating systems, it is always best to use a phased approach. At the end of each phase, and before the start of the next, the entire system should be working the same as, or better than, it was working before. Between each phase, a checkpoint can be made.

Given these considerations, an approximate order of migration might be:

1. Migrate file servers with users' personal shares. Use the Winbind program to point to an existing Windows domain controller.
2. Migrate file servers with group or team shares.
3. Migrate print servers.
4. Migrate domain controllers, if necessary.

The team that wrote this Redpaper

This Redpaper was produced by a team of specialists from around the world working at the International Technical Support Organization, Austin Center.

Stephen Hochstetler is a Consulting IT Specialist at the International Technical Support Organization, Austin Center. He writes extensively and teaches IBM® classes worldwide on all areas of system management and Linux. Before joining the ITSO three years ago, Stephen worked in the Tivoli® Services organization as a Network Management Specialist. He is a certified ITIL Service Manager.

Omkhar Arasaratnam is an IT Specialist with IBM Global Services in Canada. As an IT Specialist, he provides system administration and solution architecting services using Linux. He has more than five years of experience with Linux and uses Gentoo, SuSE, and Red Hat. His areas of expertise include Windows to Linux server migrations and security.

Rodrigo Castello Branco is a Senior Analyst in Brazil. He has five years of experience working with Linux and two years working with Domino® on Linux. His areas of expertise include Lotus® Domino administration and security, Microsoft Windows NT® and 2000 environment administration, and Citrix metaframe administration. He works at Cyberlynxx, an IBM Business Partner.

Thanks to the following people for their contributions to this project:

Andrew "tridge" Tridgell and the Samba-3 team. With talent and perseverance, they have truly succeeded in "Opening Windows to a wider world."

Michael MacIsaac
IBM Poughkeepsie

Julie Konvicka
Linux Technology Center, IBM
Austin, TX

Become a published author

Join us for a two- to six-week residency program! Help write an IBM Redbook dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You'll team with IBM technical professionals, Business Partners and/or customers.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you'll develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our papers to be as helpful as possible. Send us your comments about this Redpaper or other Redbooks™ in one of the following ways:

- Use the online **Contact us** review redbook form found at:

  ibm.com/redbooks

- Send your comments in an Internet note to:

  redbook@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. JN9B Building 003 Internal Zip 2834
  11400 Burnet Road
  Austin, Texas 78758-3493

1

Introduction

Within the IT community today, there is large install base of Windows NT servers. Microsoft has notified customers that December 31, 2004 will be the last day that Windows NT is officially supported. No longer is there a question of *if* Windows NT servers will have to be migrated to a new platform. The question now is *when* will you perform the migration and to *what*?

Regardless of whether the decision is to migrate to Windows 2000, Windows 2003, or Samba on Linux, the transition cost will be similar because the tasks are similar. The key is, how will migrating to any of these platforms effect the existing infrastructure, and what are the operating costs after the transition? Looking at both the short-term project costs of the migration and the yearly maintenance and license costs will help you to make an informed business decision.

In order to realize the full benefits of Windows 2000 or Windows 2003, Microsoft recommends implementing Active Directory, as opposed to remaining in a domain-based environment. As any architect will tell you, the more things you change, the more things can go wrong. Migrating existing domains to Active Directory requires a significant redesign of existing architecture. This translates into a higher cost.

With Samba, the customer can decide how aggressive their upgrade will be. All of the benefits of Samba can be realized without redesigning the entire infrastructure to accommodate Active Directory. You can keep your existing Windows NT domains running under Samba indefinitely if that is the strategy that you choose.

Several studies have proven that running Linux will reduce the total cost of ownership (TCO) for each server. Samba has also out performed Windows on many benchmarks (see “Related publications” on page 25). By performing more efficiently and maintaining a lower TCO, Samba on Linux has a lower operating cost than maintaining the equivalent services on Windows.

The key to Samba is flexibility. Samba is written with open standards and maintainability in mind. The life cycle of Windows NT is finite; Microsoft will withdraw support, and migrations must be planned. Samba and Linux provide an alternate that embraces open standards.

1.1 About Samba

Samba has come a long way from Andrew Tridgell's first attempts of a Server Message Block (SMB) Server on Pathworks in 1991. Today's Samba-3 provides SMB and Common Internet File System (CIFS) based file and print sharing, as well as Active Directory integration and user authentication, on a wide variety of hardware platforms. From small IBM @server xSeries® Intel®-based servers to zSeries® mainframes, Samba is, to quote the official Web site, "Opening Windows to a wider world."

There are three main functions provided by Windows NT in a network environment:

File server In this scenario, Windows NT is set up as a central file repository for enterprise-wide sharing of files or for hosting end-user home directories.

Print server Under this configuration, the Windows NT server is attached to one or more printers and configured to act as a print queue to allow multiple users access to shared printers.

Authentication server This is the most common use of Windows NT. Here, Windows NT is set up as a domain controller. It is used to authenticate users as they log on to the network. This permits access to shared resources and provides a central point to verify user credentials.

This paper describes how to migrate these functions from a Windows NT platform to Samba Version 3.0 on Linux.

Note: Many people wonder how the name "Samba" came to be. Andrew Tridgell wanted to call it SMB Server. However, another company already had a copyright for this name. At a loss for a name for his new software, Andrew resorted to the following UNIX® command to help his search:

```
$ grep -i '^s.*m.*b' /usr/dict/words
```

This searched his local dictionary for any words beginning with "s", followed by "m", and then "b". This returned the following list:

```
salmonberry
samba
sawtimber
scramble
```

Andrew picked samba, and the rest is history.

1.2 Why Samba?

Reasons to pick Samba over Microsoft operating systems to provide file, print, and authentication services include:

- Licensing costs. With Microsoft products, you must pay licensing costs per server, as well as a client access license (CAL) for every client that accesses your server.
- Heterogeneous clients. Samba allows a heterogeneous environment containing Mac OS X, Windows, Linux, and AIX® to share files and printers, as well as provide a standard method of authentication.

- Increased stability. By basing servers on Linux platforms, we also reduce the total cost of ownership (TCO) of these servers by moving from a Windows platform. Although security patches will always be required, no matter which operating system is used, the number of patches that require a reboot, and thus an outage, under Linux are significantly less than those under Windows. This creates greater uptime and fewer disruptions of service.
- Improved performance. Samba has been proven to out perform Windows when providing these services. Samba V2.2 has a history of easily defeating Windows 2000 in synthetic benchmarks, as well as real world workloads. Samba-3 is continuing in this tradition and has out performed Windows 2003 by as much as 2.5 times in an early benchmark.[1] Although any benchmark can be proven or disproven using various hardware and drivers, this benchmark of untuned servers does give you an indication of the out-of-box performance that Samba brings to your business. Many customers want to use Samba to provide enhanced the performance and a longer life cycle to their current hardware.

Regardless of your reasons for choosing Samba, this paper assists in providing a high-level overview of what services Samba provides and ideas of how to implement them in an enterprise environment.

Note: This paper is meant to introduce some of the concepts and best practices associated with implementing Samba-3. It is not meant as a “How To.” This is out of the scope of this paper. For in-depth technical explanations regarding Samba and its features, see the Samba Web site, available at:

http://www.samba.org

The *Samba HOWTO Collection* for Version 3.0 is available at:

http://us1.samba.org/samba/docs/Samba-HOWTO-Collection.pdf

[1] http://www.itweek.co.uk/ITWeek/itw_graph_1144289.jsp

2

Samba file services

In this chapter, we discuss the following topics:

- Providing DFS™ services in 2.1, “DFS” on page 6
- Providing file shares in 2.2, “File shares” on page 7
- Limitations in the Samba implementation of SMB/CIFS in 2.3, “Limitations” on page 8

The choice of which product should supersede a Windows NT file server is a daunting one. From a feature perspective, Samba and Windows 2003 are evenly matched. As previously stated, the main benefits of Samba are flexibility and performance. A recent benchmark cited that an untuned Samba out performed an untuned Windows 2003 server by more than 2.5 times. With any benchmark, you will probably be able to find hardware and driver combinations that allow each software to win that particular benchmark. However, this benchmark does provide an indication of the out-of-the-box capabilities of Samba that will give you a quick return on investment (ROI) without a lot of expensive administrator tuning. Coupled with the TCO advantages of using a Linux server over a Windows server, the choice seems clear.

Samba can serve traditional file shares (SMB/CIFS) and Distributed File System (DFS) shares transparently to clients. Samba can also authenticate user privileges in either Active Directory-based or domain-based environments, as described in Chapter 4, “User authentication” on page 19.

Samba provides SMB/CIFS, as well as DFS services to Windows clients. This chapter describes how to enable each, and the caveats associated with implementation of these features through Samba on Linux.

2.1 DFS

Distributed File System (DFS) was introduced in Windows 2000. With DFS, geographically disconnected file servers appear as part of the same hierarchy, as shown in Figure 2-1.

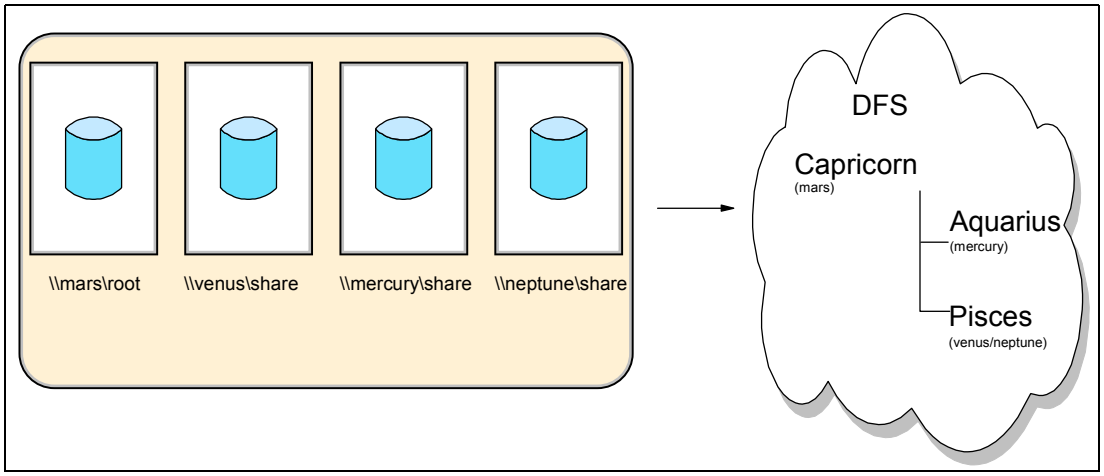

Figure 2-1 DFS example

In this diagram, you can see how the separate file spaces on different physical servers have been represented contiguously under the DFS hierarchy.

2.1.1 Prerequisites

In order to use Samba for DFS, the Samba package has to be compiled with the **`--with-msdfs`** option. This is standard on most distributions. If your distribution does not have this option compiled into its package, obtain the source code from the Samba Web site and recompile the package from source:

`http://www.samba.org`

2.1.2 Configuration

After the package has been configured in this manner, add **`host msdfs = yes`** in the smb.conf file and restart the smbd and nmbd services. After verifying that the Samba daemons start without issue, you can configure the DFS root.

On a Linux system, the DFS root contains symbolic links to the other file spaces. Example 2-1 shows an example of how to configure the smb.conf file of the root DFS server.

Example 2-1 smb.conf: From DFS example

```
# Example DFS enabled smb.conf
[global]
   netbios name = CAPRICORN
   host msdfs = yes
[dfs]
   path = /export/dfsroot/
   msdfs root = yes
```

Example 2-2 on page 7 shows how to configure the remaining branches of the DFS tree from Example 2-1.

Example 2-2 Adding the remaining branches of the DFS tree

```
root# cd /export/dfsroot
root# chown root /export/dfsroot
root# chmod 755 /export/dfsroot
root# ln -s msdfs:mercury\\share aquarius
root# ln -s msdfs:venus\\share,msdfs:neptune\\share pisces
```

In our example, the shared directory on mercury is mounted under a DFS branch called aquarius, and pisces is a load-balanced branch between neptune and venus.

Tip: In our testing, we found that it is critical that the path on the root DFS server is lowercase.

For example, the following will fail:

```
path = /export/DFSroot/
```

But, this works well:

```
path = /export/dfsroot/
```

2.2 File shares

SMB and CIFS shares are the most common file shares provided by Samba. These shares are accessible through the Universal Naming Convention (UNC), for example:

```
\\servername\sharename
```

Or:

```
\\w.x.y.z\sharename
```

Example 2-3 shows an example of how to add a file share to an existing smb.conf file.

Example 2-3 smb.conf: Providing a simple file share

```
[share]
   path = /export/smb/data
   comment = Data Directory on Capricorn
   read only= yes
   valid users = @workers
   write list = manager
```

This exports the data from our directory as a share. In this particular case, because the name of the server is Capricorn, the share can be accessed by \\CAPRICORN\DATA. The valid users line only permits the user belonging to the group workers to read this data. The user named manager is allowed to write to the share.

Note: For information about how to authenticate users, see Chapter 4, “User authentication” on page 19.

2.3 Limitations

There are some limitations in the Samba implementation of SMB/CIFS: some of them are because Samba is running on a Linux file system, others are because SMB/CIFS is a closed standard. The limitations include:

NTFS permissions The NTFS file system can support about 13 different permissions based on the NTFS security model. Some do not map directly to the file permission scheme used by Linux.

Multiple owners/groups The Windows security model enables multiple users and groups to have permissions related to a file. The Linux permission scheme only allows one owner and one group.

Take Ownership button Samba does not support the “Take Ownership” button due to its reliance on root permissions.

3

Samba print services

In this chapter, we discuss the following topics:

- Setting up CUPS in 3.1, “Configuring CUPS” on page 10
- Samba and CUPS integration in 3.2, “Configuring Samba to print through CUPS” on page 18

Windows NT servers have long been used in departments as a centralized method of sharing printers. Samba, with Common UNIX Print System (CUPS), can easily replace these existing servers. Samba also provides advanced functions such as printer driver distribution, which is also an improved function in Windows 2000 and later.

Samba also extended its print capabilities to provide Active Directory printer capabilities, plus other key Active Directory print features, that allow Samba to integrate into existing Active Directory environments.

These robust print features can be integrated into an existing Samba file server, or in demanding environments, be deployed on a stand-alone server as an easily configured high-performance print server.

Samba not only enables file sharing, but also enables users to share printers across the network. Advanced Samba print configurations also allow for load balancing and fail-over in the event that a physical print device goes down.

3.1 Configuring CUPS

Common UNIX Printer System (CUPS) has quickly become the de facto standard for printing under Linux. It has hundreds of print drivers in its library.

Most Samba installations rely on CUPS to communicate with the physical printer. This symbiotic relationship is so common that we chose to cover a CUPS and Samba configuration in this paper.

Most major distributions ship with CUPS. If yours does not, you can obtain the appropriate package or source code and installation instructions from:

`http://www.cups.org`

After installing the CUPS package and starting cupsd, you can configure CUPS by pointing your browser to `http://localhost:631`.

The following figures show CUPS pages that illustrate how to configure a printer with CUPS. Figure 3-1 shows the main CUPS page.

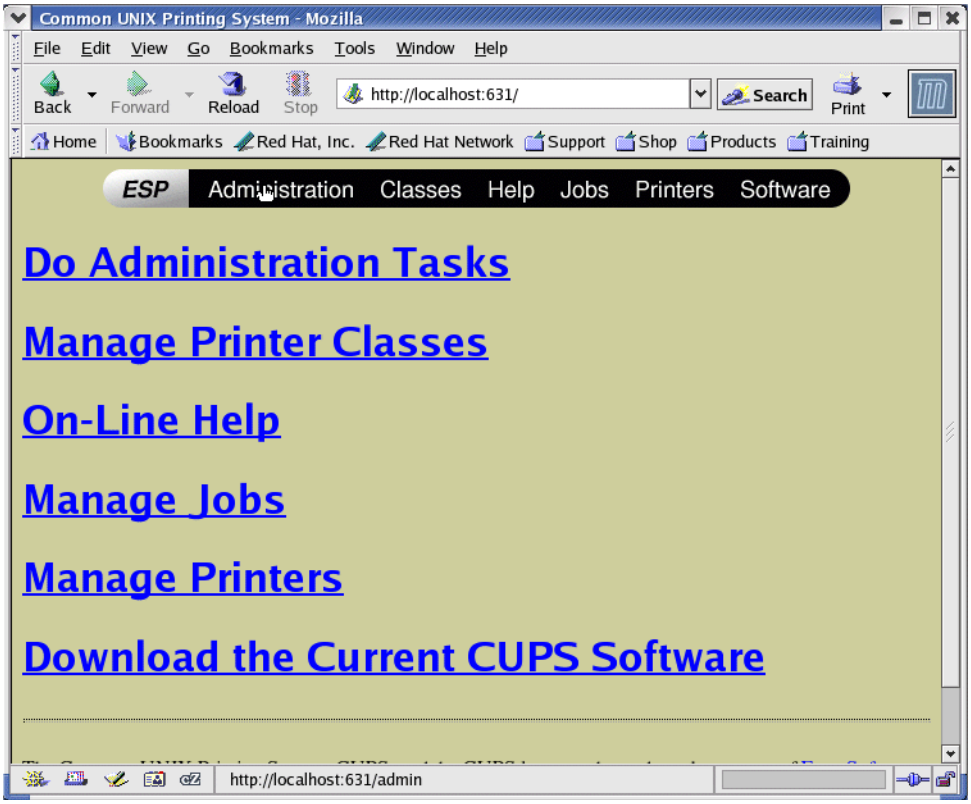

Figure 3-1 The main CUPS page

To configure a printer:

1. After selecting **Printers**, you are able to add a new printer, as shown in Figure 3-2.

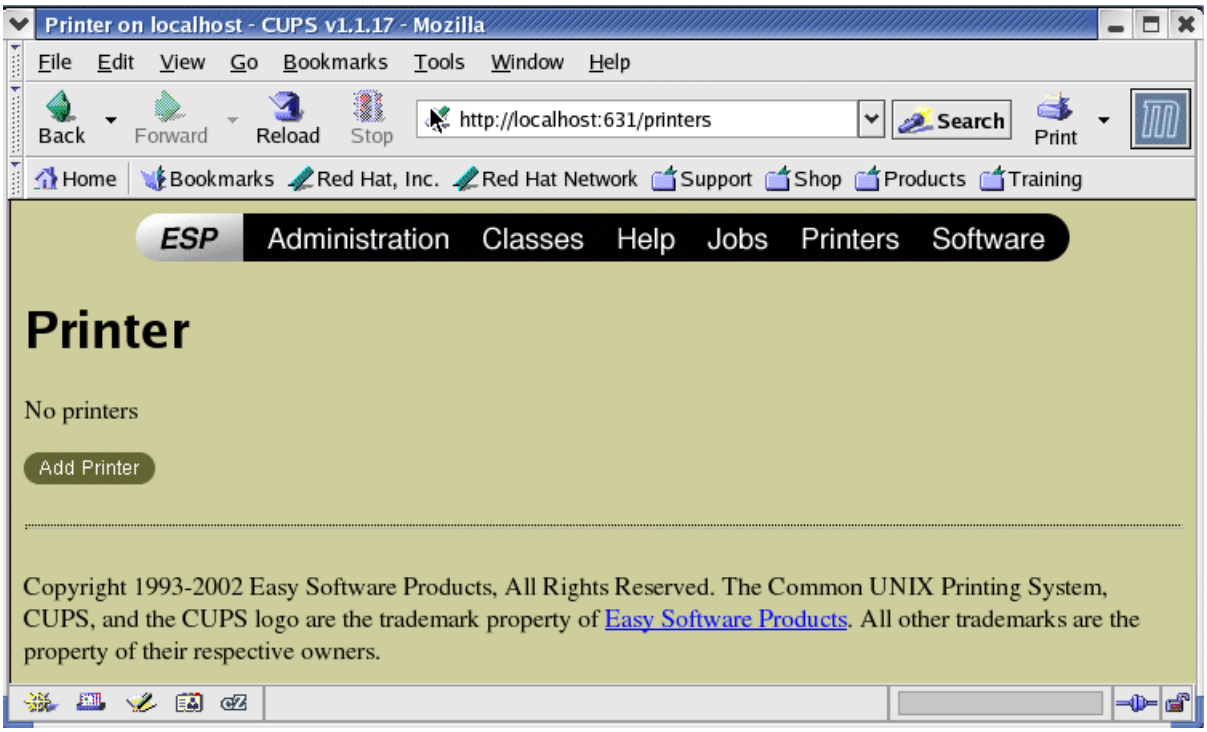

Figure 3-2 Add Printer page

2. Edit basic information such as printer name, location, and description, as shown in Figure 3-3 on page 12.

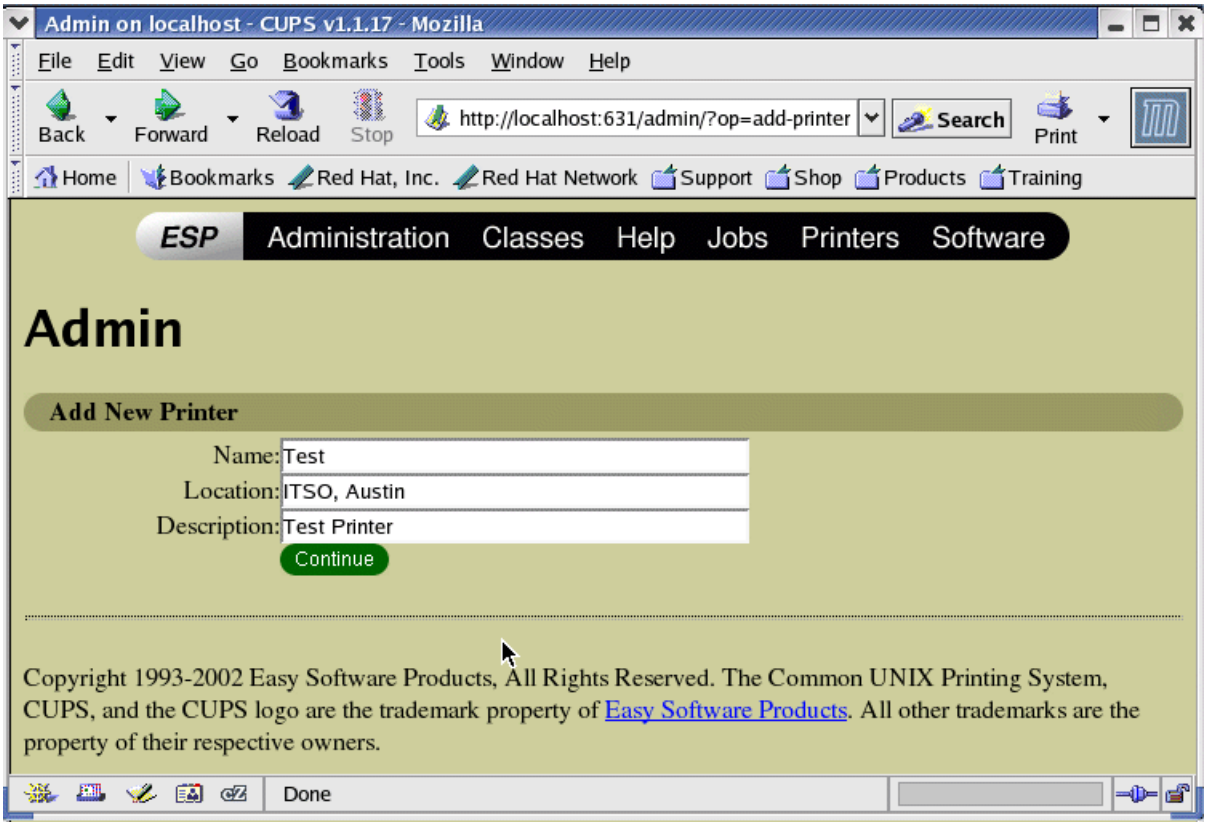

Figure 3-3 Basic printer information

3. After clicking **Continue**, select the type of device, as shown in Figure 3-4 on page 13.

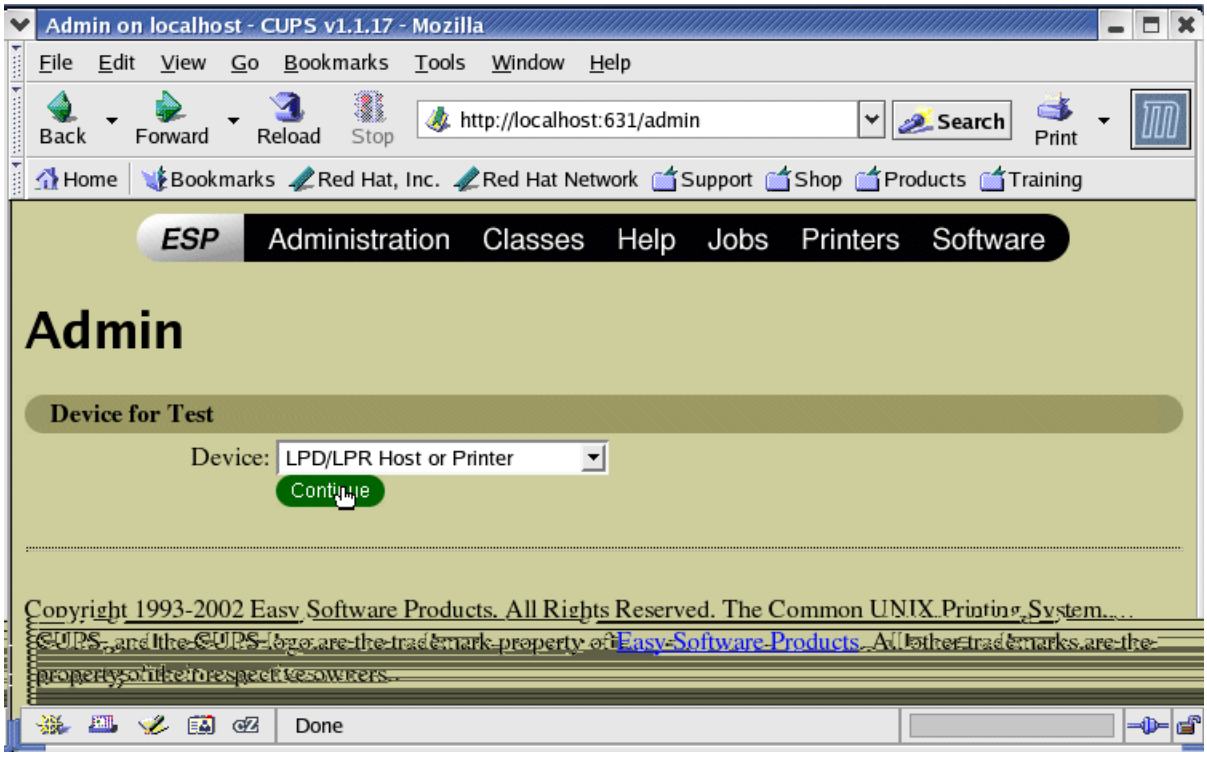

Figure 3-4 Device type

4. After clicking **Continue**, specify the location of the printer, as shown in Figure 3-5 on page 14.

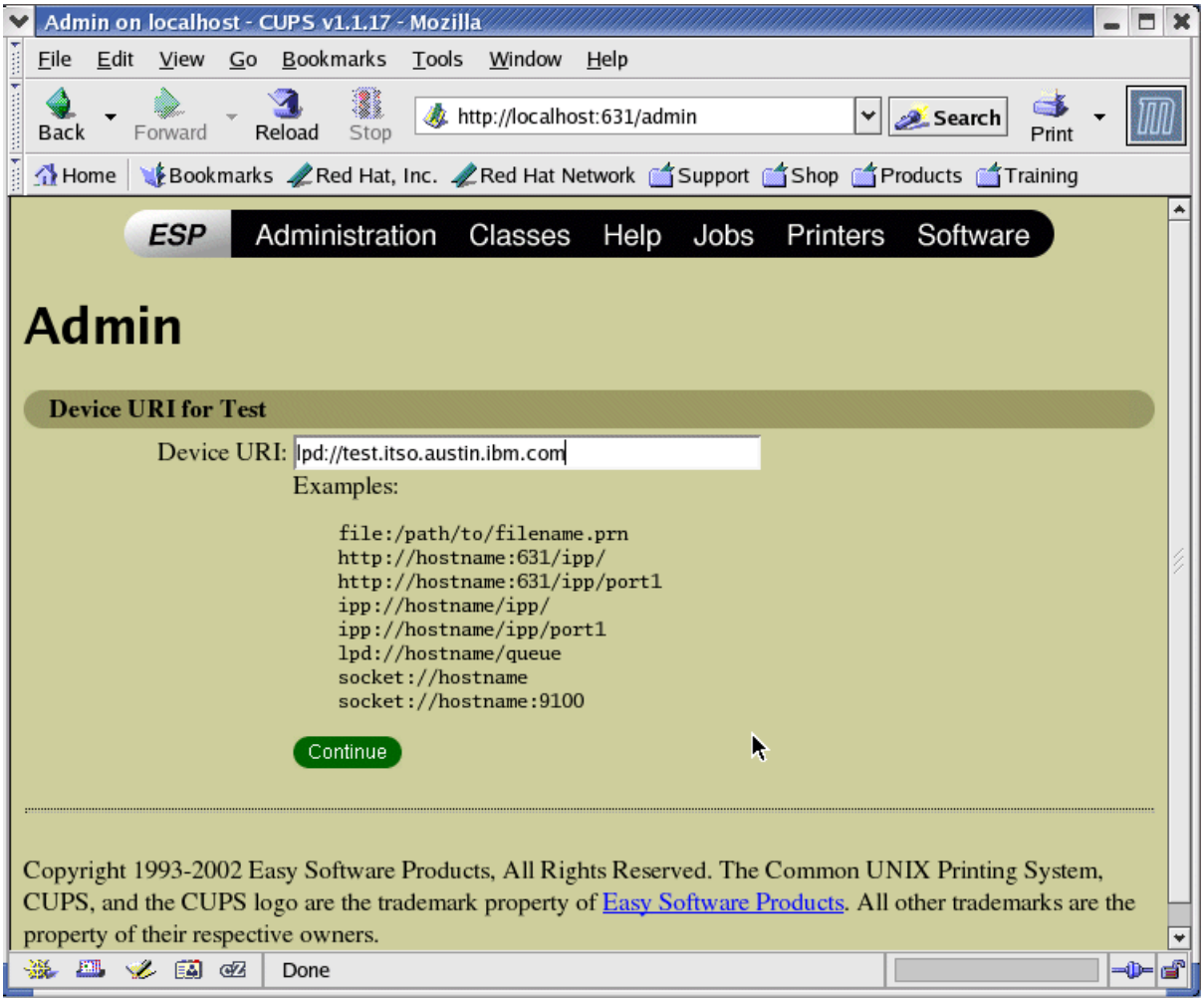

Figure 3-5 URI to printer/print queue

5. After clicking **Continue**, select the make of the printer, as shown in Figure 3-6 on page 15.

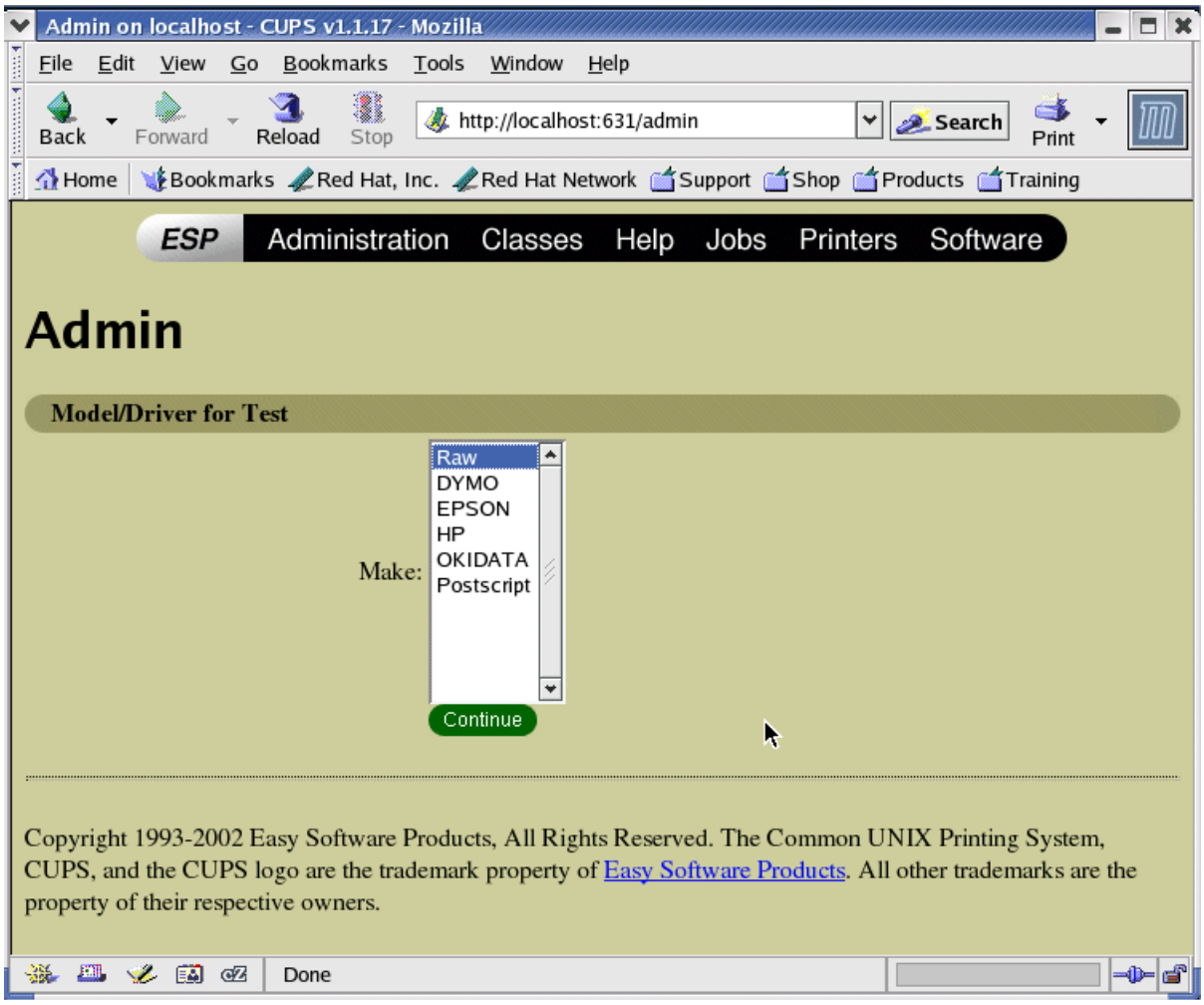

Figure 3-6 Printer make

6. After clicking **Continue**, select the model, as shown in Figure 3-7 on page 16.

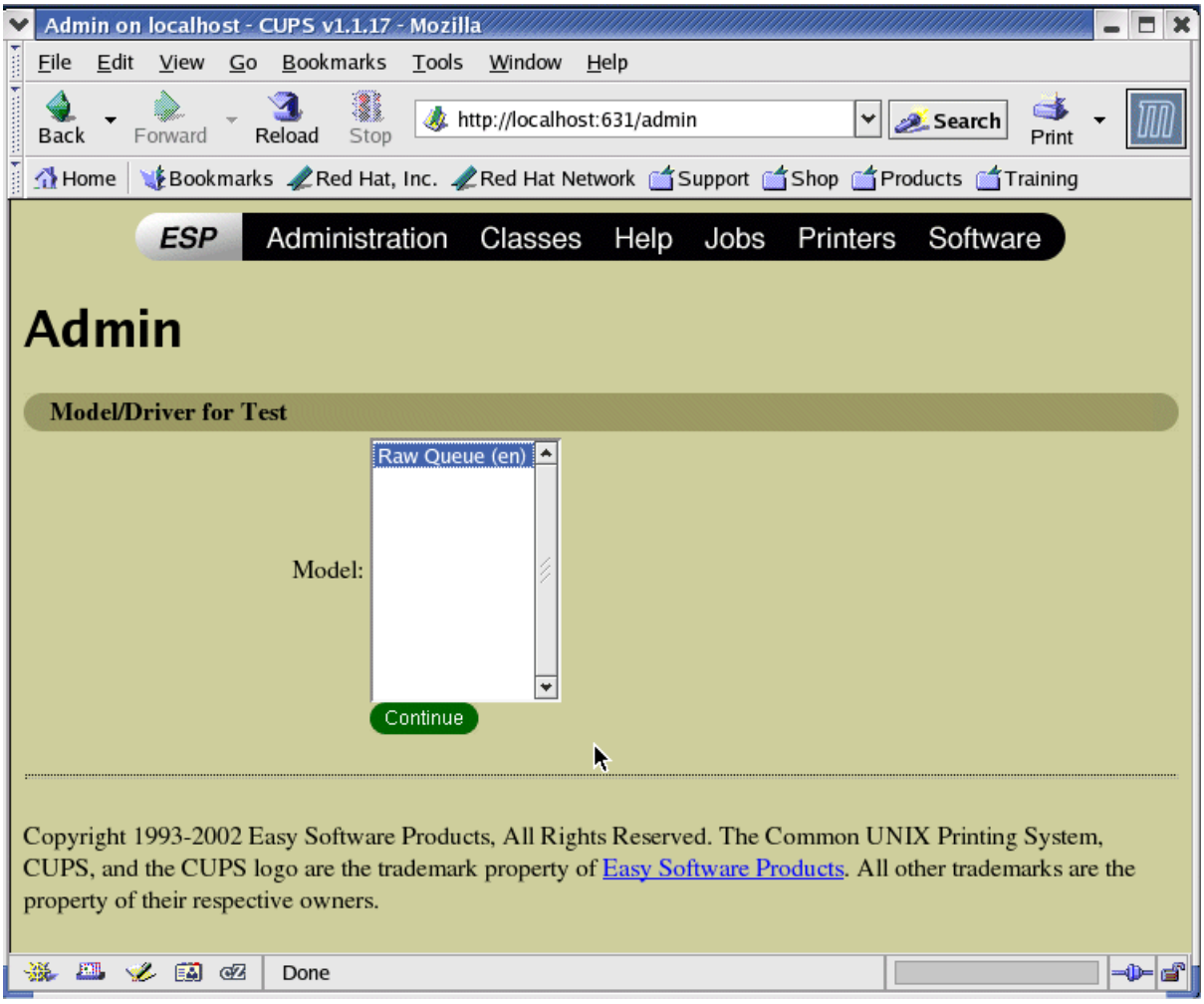

Figure 3-7 Printer model

7. After clicking **Continue**, the success page opens, as shown in Figure 3-8 on page 17.

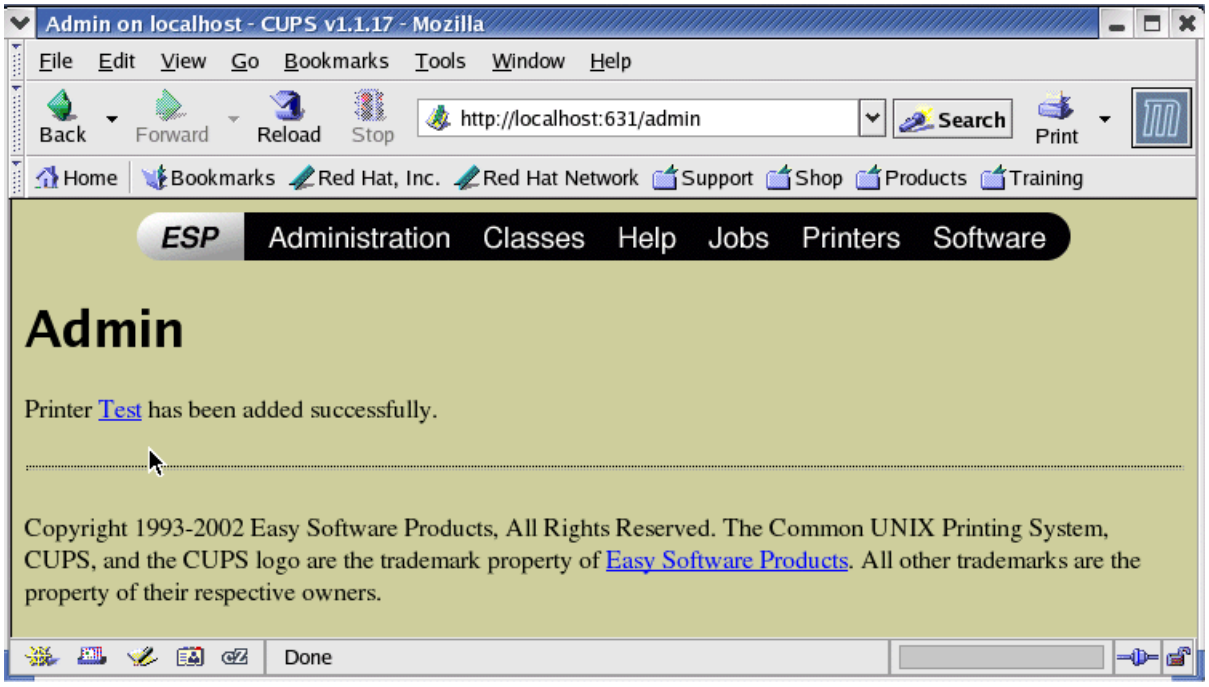

Figure 3-8 Success message

Figure 3-9 shows what the printer page looks like with a configured printer.

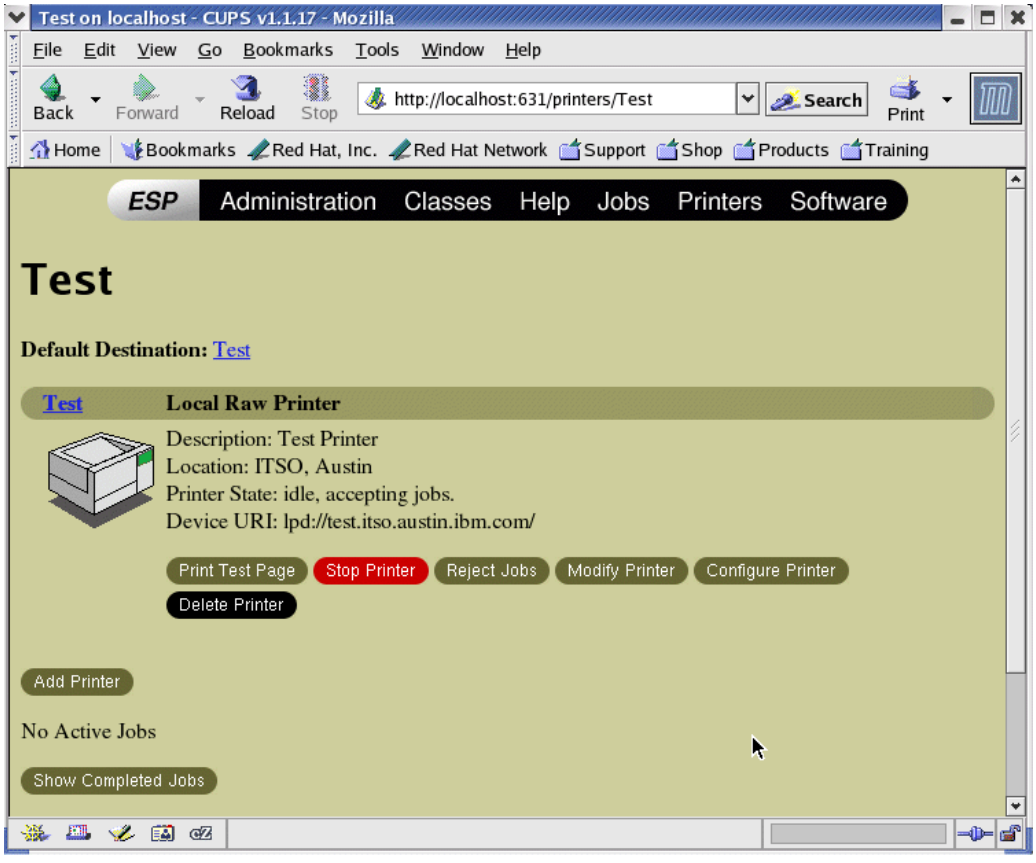

Figure 3-9 CUPS printer status page

3.2 Configuring Samba to print through CUPS

Configuring Samba to send its print jobs to CUPS is straightforward. Example 3-1 shows a the settings in the \etc\smb.conf file.

Example 3-1 smb.conf: For simple print serving

```
[global
   ....
   printcap name = cups
   printer admin = admin
   printing = cups

[printers]
   path = /var/lib/samba/printers
   create maske = 0600
   printable = yes
   browseable = no
```

After adding these lines, restart the Samba daemons. You can then add the Samba printer to any Windows client as though it were a Windows-based network printer.

Tip: It is possible to have the driver for your printer automatically provided to Windows clients, but that is out of the scope of this paper. A comprehensive guide of how to accomplish this is available at:

http://acd.ucar.edu/~fredrick/linux/samba-printer

4

User authentication

In this chapter, we discuss the following topics:

- Active Directory integration in 4.1, “Active Directory” on page 20
- Domain integration in 4.2, “Domain” on page 22
- Local authentication in 4.3, “Local authentication” on page 22

Domain and Active Directory integration has long been a goal of Samba. With Samba-3, the development team has succeeded in creating a program that can replace a primary domain controller (PDC) or backup domain controller (BDC).

The Samba team has also gone further, to integrated enterprise-capable back ends such as LDAP and MySQL for the storage of user information. This results in higher availability of domain services.

Samba will also allow domains and the domain hierarchy to be maintained well after Windows NT is declared end of life by Microsoft. This way, IT departments can migrate existing domains to Samba.

It’s important to remember that migrating from Windows NT to Windows 2003 is no easier than migrating to Samba under Linux. Microsoft recommends rebuilding the servers that will be hosting the Windows 2003 operating system, as opposed to doing an upgrade. From a project perspective, this results in the same amount of time being invested in transition, regardless of the platform chosen.

One of the key reasons that Linux is preferred is the meager hardware requirements. Microsoft recommends that Windows 2003 domain controllers have at least 1 GHz Xeon processors with 1 GB of RAM and at least 30 GB of hard disk drive space. Conversely, Samba can be run on much older systems with less than half the speed and capacity of the Windows 2003 requirements.

There are three main ways that Samba can authenticate users: Active Directory, domain, and local authentication. We describe all three in this chapter.

4.1 Active Directory

User-level access can be implemented by instructing Samba to look to a domain controller (DC) for user authentication. With its latest release, Samba can now fully integrate into an Active Directory environment using LDAP/Kerberos to authenticate users.

In order to use user level authentication, Samba uses Kerberos. The strength of Kerberos is that it allows a server such as Samba to authenticate a user without talking to the DC. It does this by checking if it can decrypt the client's service ticket using the secret that Samba and the KDC share. If it can be decrypted, Samba knows that the client must have obtained that service ticket from the KDC. This requires several steps. Example 4-1, Example 4-2, and Example 4-3 show a brief example that allows our server, SAMBA, to authenticate against DC W2KDOMCTL in the WIN2KDOM domain.

Example 4-1 smb.conf: For Active Directory integration

```
[global]
   realm = WIN2KDOM
   security = ads
   password server = W2KDOMCTL
```

Example 4-2 krb5.conf: For Active Directory integration

```
[libdefaults]
   default_realm = WIN2KDOM
   default_etypes = arcfour-hmac-md5
   default_etypes_des = arcfour-hmac-md5

[realms]
   WIN2KDOM = {
   kdc = W2KDOMCTL
   }
```

Example 4-3 /etc/hosts file: Optional part of Active Directory integration

```
# NOTE: This entry is unnecessary if your DNS server supports reverse lookups
w.x.y.z W2KDOMCTL
```

After implementing these changes, verify that Kerberos is configured properly by authenticating as the Administrator, as shown in Example 4-4.

Example 4-4 Verify Kerberos configuration

```
# klist -e
# kinit Administrator@WIN2KDOM
Password for Administrator@WIN2KDOM:
```

Note: The realm statement in krdb5.conf must be all uppercase; otherwise, you will get an error message stating that a KDC cannot be found for the realm.

Note: Kerberos is extremely time dependant. Either synchronize the clocks on both servers, or synchronize both against a Network Time Protocol (NTP) server, so that their times are synchronized.

After you confirm the Kerberos connectivity, join SAMBA to the Active Directory, as shown in Example 4-5 on page 21.

Example 4-5 Joining SAMBA to an existing Active Directory

```
# net ads join -U Administrator%password
Using short domain name -- WIN2KDOM
Joined 'SAMBA' to realm 'WIN2KDOM'
```

Note: We observed that sometimes the Administrator password would not authenticate. It seems that this is a known issue and the Administrator password must be changed at least once (after installation) before we can authenticate in this manner. This might be resolved in a future release of Samba.

On the domain controller, you will see that SAMBA has joined the Active Directory, as shown in Figure 4-1.

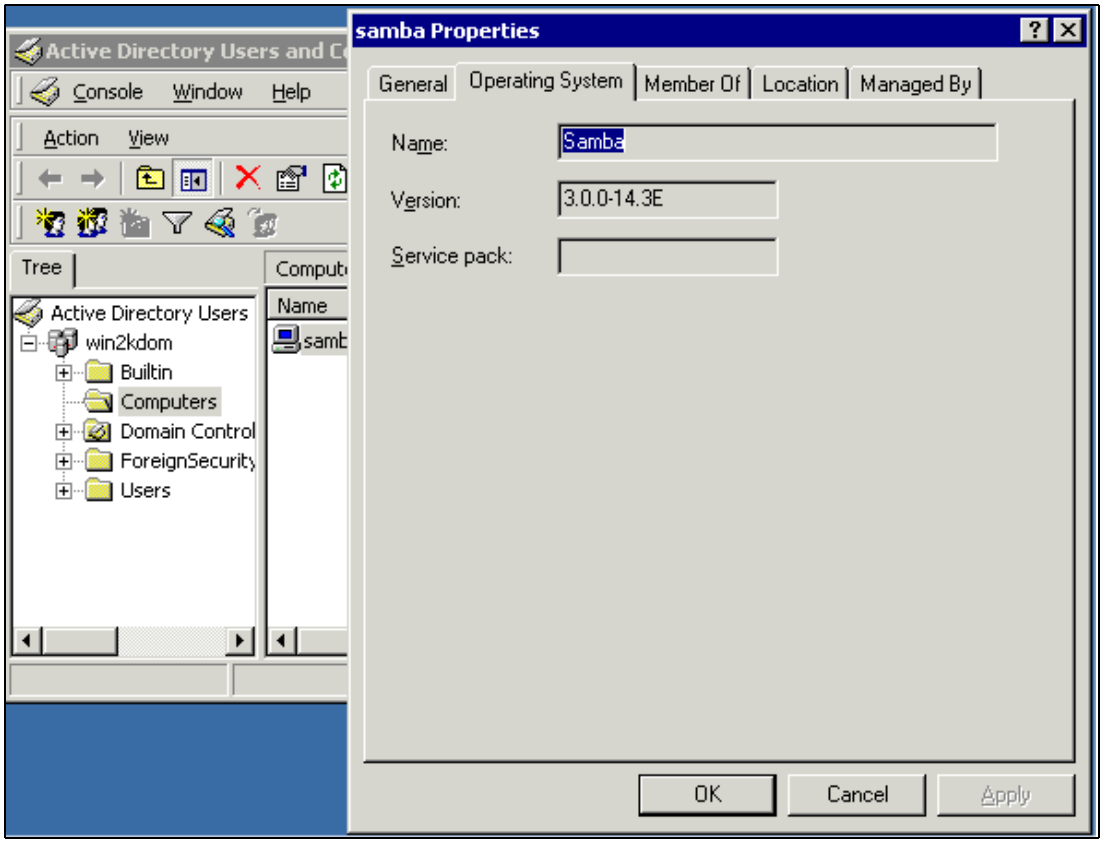

Figure 4-1 Samba running in a native Active Directory

Next, verify that you can see all of the users in the domain using the command shown in Example 4-6.

Example 4-6 Verifying users in the domain

```
#net ads user
Administrator
Guest
TsInternetUser
IUSR_W2KDOMCTL
IWAM_W2KDOMCTL
krbtgt
```

4.2 Domain

It is possible to configure Samba to connect to legacy domains as well if your infrastructure has not yet been upgraded to Active Directory. Example 4-7, Example 4-8, and Example 4-9 show a brief example that illustrates how to join SAMBA in domain mode.

Example 4-7 smb.conf: For domain authentication

```
[global]
   workgroup = WIN2KDOM
   netbios name = SAMBA
   security = DOMAIN
   encrypt passwords = yes
   password server = *
   winbind uid = 10000-20000
   winbind gid = 10000-20000
   winbind separator = +
   winbind enum users = yes
   winbind enum groups = yes
```

Example 4-8 lmhosts file: Required for domain authentication

```
w.x.y.z WIN2KDOM
w.x.y.z W2KDC
```

Example 4-9 nsswitch.conf: Required for domain authentication

```
passwd: files winbind
group: files winbind
```

After implementing these changes and restarting SAMABA, SAMBA must be joined with the domain. This can be accomplished by executing the command shown in Example 4-10.

Example 4-10 Joining a domain

```
# net rpc join -U Administrator%password
Joined domain WIN2KDOM
```

After the Samba server has been registered against the domain, start winbindd. In order to verify that winbindd is configured correctly, try running the command shown in Example 4-11.

Example 4-11 Verifying that winbindd is working

```
wbinfo -t
checking the trust secret via RPC calls succeeded
```

4.3 Local authentication

Samba is capable of acting as a primary domain controller (PDC) or a backup domain controller (BDC) in a domain environment. The Security Account Manager (SAM) information can be stored and managed by a number of methods. Samba-3 currently supports smbpasswd, tbdsam, ldapsam_compat/ldapsam, and mysqlsam.

Restriction: With Samba-3, Samba cannot be a BDC to a PDC that is running Windows NT 4.0.

smbpasswd

The simplest way to implement Samba in a small environment is to implement user authentication through an smbpasswd file. This file is used to maintain the user IDs and passwords of all users that are accessing data on the server through Samba. This particular method of account information storage is plagued by being difficult to replicate and therefore is not recommended for PDC/BDC environments. As the user base increases, smbpasswd also becomes exceedingly difficult to manage due to administration overhead. In general, smbpasswd should be avoided for all but the simplest Samba implementations. There are signs that this method of authentication might depreciated in future releases; it is recommended to move away from it.

tdbsam

This back end was created for Samba-3 in response to the limitations imposed by smbpasswd in Samba V2. tdbsam stores all of the same data captured by smbpasswd, along with additional SAM information. This is all stored in a trivial database (TDB) format. The Samba development team recommends this for sites with less than 250 users. Because this data is stored locally, tdbsam is not recommended for large sites, or sites that require PDC/BDC replication.

ldapsam_compat/ldapsam

The LDAP capabilities are of particular interest here. With an LDAP back end, Samba-3 servers can function in a true PDC/BDC relationship. Ideally, a master LDAP server would be used with the PDC. The BDCs would then communicate with slave LDAP servers. The consistency of the LDAP user data would be maintained by the strong replication capabilities of LDAP. ldapsam_compat is provided as a backwards compatibility while older Samba schemas are updated in the LDAP environment. ldapsam is recommended for environments with more than 1000 users or environments where BDCs are required because of WAN links or other mitigating factors.

Note: Your existing LDAP schema might need to be modified to accommodate Samba. For which attributes need to be added, refer to the examples/LDAP in the source distribution or the Samba documentation, available at:

http://www.samba.org

Example 4-12 shows how to set up Samba to perform LDAP back-end authentication.

Example 4-12 smb.conf: For DC with LDAP back end

```
[globals]
   workgroup = SAMBADOM
   passdb backend = ldapsam://slave.ldap.com
      ldapsam://master.ldap.com
   domain master = yes
   domain logons = yes
```

Tip: In this particular scenario, we assume that one of the LDAP servers is geographically closer (slave.ldap.com) and have therefore shown preference to querying this server.

Note: We recommend that you use Transport Layer Security (TLS) to encrypt LDAP queries between the LDAP back end and the Samba DC, as well as during LDAP replication, because sensitive data might be transferred.

mysqlsam

This back end leverages the popular open source database MySQL for storing its data. mysqlsam is recommended as a middle ground between ldapsam and tdbsam. Although its method of storing data is not recommended for BDC environments, it is quite robust and is recommended when serving between 250 and 1000 users.

Note: The MySQL database used must confirm to a specific schema. For information about how to establish this schema, see examples/pdb/mysql/mysql.dump in the source distribution or the Samba Web site, available at:

http://www.samba.org

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this Redpaper.

IBM Redbooks

For information about ordering these publications, see “How to get IBM Redbooks” on page 26. Note that some of the documents referenced here may be available in softcopy only.

- *Deploying Samba on IBM eServer Blade Center*, REDP-3595
- *Implementing Linux in Your Network Using Samba*, REDP-0023
- *Linux on IBM eServer zSeries and S/390: Managing a Samba Server from z/VM*, REDP-3604
- *Samba Installation, Configuration, and Sizing Guide,* SG24-6004

Other publications

These publications are also relevant as further information sources:

- *Migration Guide: A guide to migrating the basic software components on server and workstation computers*, KBSt Publication Series, Volume 57, July 2003, ISSN 0179-7263, available at:

  http://www.kbst.bund.de/Anlage303777/pdf_datei.pdf
- Terpstra, John H., and Jelmer R. Vernooij, *The Official Samba-3 HOWTO and Reference Guide*, Prentice Hall PTR, 2003, ISBN 0131453556

Online resources

These Web sites and URLs are also relevant as further information sources:

- Samba Web site

  http://www.samba.org
- *Samba HOWTO Collection*

  http://us1.samba.org/samba/docs/Samba-HOWTO-Collection.pdf
- Samba 3 versus Windows Server 2003: File server performance comparison

  http://www.itweek.co.uk/ITWeek/itw_graph_1144289.jsp
- CUPS Web site

  http://www.cups.org
- How to set up print driver distribution

  http://acd.ucar.edu/~fredrick/linux/samba-printer
- MacIsaac, M., *Migrating Windows Servers to Samba*

  http://linuxvm.org/Present/misc/SambaMig.pdf

- The European Commission Interchange of Data between Administration (IDA) Open Source Migration Guidelines

  http://europa.eu.int/ISPO/ida/jsps/index.jsp?fuseAction=showDocument&parent=news&documentID=1647
  http://europa.eu.int/ISPO/ida/export/files/en/1618.pdf

- *Total Cost of Ownership for Linux Web Servers in the Enterprise*, Robert Frances Group, September 2002

  http://www.rfgonline.com/subsforum/LinuxTCO.pdf

- Schadler, T., *The Linux Tipping Point*, March 2003

  http://www.linuxleap.com/ForresterLinuxTippingPoint.pdf

- Vianney, D., *Hyper-Threading speeds Linux*, January 2003

  http://www.ibm.com/developerworks/linux/library/l-htl/

- Sherman, R., *Oracle 9i on Linux vs. Windows 2000 Server*

  http://www.interealm.com/technotes/roby/pentmark.html

- Carr, N., J. Hogan, and J. Opp, *Benchmarks prove the performance of the Red Hat Enterprise Linux platform*, October 2002

  http://www.redhat.com/whitepapers/rhel/ASBenchmarkWhitePaperigPDFredv2.pdf

How to get IBM Redbooks

You can search for, view, or download Redbooks, Redpapers, Hints and Tips, draft publications and Additional materials, as well as order hardcopy Redbooks or CD-ROMs, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Open Your Windows with Samba on Linux

Redpaper

Linux requires fewer critical security updates

Describes the just released Samba-3 with enhanced features

Linux can lower your total cost of ownership

The Windows NT software that has provided file sharing and print servers for your business will soon become an end-of-life product that is no longer supported through normal channels. Your business demands a supported infrastructure, thus a migration to a new network operating system is inevitable.

Samba-3 is the latest software that provides file and print services for Microsoft Windows clients. These services can be hosted from any TCP/IP-enabled platform. The Samba project includes not only an impressive feature set in file and print serving capabilities, but also has been extended to include client functionality, utilities to ease the migration to Samba, tools to aid interoperability with Microsoft Windows, and administration tools.

Now is your opportunity to set a new course of openness and choice for your IT infrastructure, while reducing the cost of client licenses. Embrace the benefits of open source software by choosing Samba on Linux to replace your end-of-life Windows NT environments.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks