IBM

File and Print Serving with Linux on IBM @server i5

- Learn the benefits of migrating file and print serving workloads using Linux on @server i5
- Replace Microsoft Windows-based services with Linux Samba
- Create a coexistence of Active Directory Server and Linux Samba

Yessong Johng
Sandra Cabral
Arnaldo Chaim
Livio Teixeira Filho
Charlie Quigg

Redpaper

ibm.com/redbooks

International Technical Support Organization

File and Print Serving with Linux on IBM @server i5

November 2005

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

First Edition (November 2005)

This edition applies to i5/OS V5R3 and SUSE LINUX Enterprise Server 9 (SLES9).

This document created or updated on November 21, 2005.

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 5L™	eServer™	pSeries®
AIX®	IBM®	Redbooks (logo)  ™
AS/400®	iSeries™	Redbooks™
Domino®	Lotus®	Virtualization Engine™
@server®	OS/400®	WebSphere®
@server®	POWER™	xSeries®

The following terms are trademarks of other companies:

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

Intel, Intel logo, Intel Inside logo, and Intel Centrino logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States, other countries, or both.

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

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

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

Preface

This IBM® Redpaper introduces options for migrating a Microsoft® Windows®-based file and print serving workload to a Linux®-based Samba server on the IBM @server i5. It is written to help administrators who are in charge of providing file and print services to their Windows clients and who are considering such a migration project.

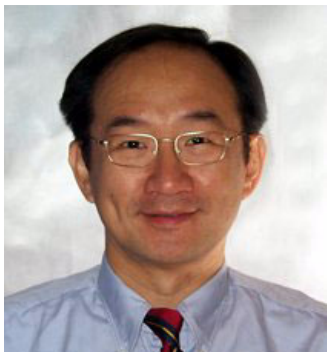
To explain the migration options, this paper presents the following three scenarios from the migration implementation perspective:

- Replacement of Windows NT®-based services of file and print serving, as well as domain controller functions, with Linux Samba
- Coexistence of the Windows-based domain controller function with Linux Samba, which provides file and print serving workload
- Coexistence of Windows-based Active Directory Server with Linux Samba

For these scenarios, you see a before and after view of the migration environment. Then you follow the migration process step-by-step, and learn about the configuration files and commands to run.

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 (ITSO), Rochester Center.



Yessong Johng is an IBM Certified IT Specialist at the IBM ITSO, Rochester Center. He started his IT career at IBM as a S/38 Systems Engineer in 1982 and has been working with the S/38, AS/400®, and now IBM @server iSeries™ for 20 years. He writes extensively and develops and teaches IBM classes worldwide on the areas of On Demand Business on iSeries. Yessong's areas of expertise include IBM WebSphere® and Lotus® Domino® implementation on iSeries, with a focus on integration. In addition, he specializes in Linux and Linux solutions on iSeries.

Arnaldo Chaim is an IT Specialist, and a UNIX® specialist, for EDS in Brazil, working on the Midrange Hosting team. He has been working in IT for 10 years and has experience in working on different platforms, including UNIX systems and network servers, as well as on different consolidation projects and deployment. Previously, Arnaldo was an administrator of technical support for Novell and Microsoft. He was also an instructor at a technical school in Brazil. Arnaldo has a degree in systems analysis.

Charlie Quigg has been an IBM technical consultant, for nine years, assisting UNIX and Windows software vendors who are interested in deploying applications on the iSeries server. Prior to his current assignment, he was a software engineer in the iSeries lab. Specifically, he worked on OS/400® implementations of UNIX-type APIs. Charlie began his career with IBM in 1981 as a technical writer. He holds two Bachelor of Science degrees, one from Winona State University in computer science and one from the University of Wisconsin-Stout in technical communications.

Livio Teixeira Filho is an IT Specialist for EDS in Brazil, working on the Midrange Hosting team. He provides technical support and problem solving for EDS customers, handling complex and critical scenarios. He has experience in working on different UNIX platforms, as well as working on many consolidation and deployment projects. Livio is certified by the Linux Professional Institute, as well as has certification in Conectiva Linux, HP-UX CSA, and IBM @server pSeries® Specialist Administration and Support for AIX® 5L™ v5.2.

Sandra Cabral has been providing technical support to members of PartnerWord for Developers for the past six years, while working in the IBM ATS organization in Rochester, MN. Her areas of expertise include: iSeries Access for Windows/Web, Linux, printers, Secure Sockets Layer (SSL), and client/server computing. Prior to that, she was an IBM Business Partner in Brazil, providing AS/400 training and integration for new accounts. Sandra holds bachelor degrees in computer science and civil engineering, as well as a master degree in organization management.

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

Erwin Earley
George Gaylord
Craig Johnson
Mike Schambureck
Kyle Wurgler
IBM Rochester

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 email to:

  redbook@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. JLU Building 107-2
  3605 Highway 52N
  Rochester, Minnesota 55901-7829

1

Migrating a Windows NT workload (PDC or BDC) to Linux on eServer i5

Microsoft announced that the company is discontinuing support for Windows NT4 and that users need to migrate their NT4-based workload to another platform. Since Microsoft's introduction of Windows NT4 servers, businesses have gradually evolved their IT infrastructure around Windows NT4. With Microsoft's announcement of phasing out support for Windows NT4, customers are left with no choice but to upgrade to a newer version of Windows. This calls for revamping the IT infrastructure because newer versions of Windows 2003 servers take a fundamentally different approach toward the basic design of domains.

To take advantage of the enhanced features in Windows 2000 or Windows 2003, these customers must adopt the Microsoft Active Directory architecture. They must also replace other infrastructure software because direct upgrades may not be possible from older versions to newer versions. Consider the example of Microsoft Exchange 5.5 to Microsoft Exchange 2002.

Linux along with one of its native applications of Samba-3 offers a practical, alternative target server for the current NT4-based file and print serving environment. This chapter explains how to perform a migration from a Windows NT4 Domain Control and file and print server, running on a stand-alone Intel® server, to Linux with Samba-3 based domain controller on @server i5.

1.1 Understanding the migration workload

This migration provides an opportunity for you to revise and update roaming profile deployment and folder redirection. Given that you must port the greater network configuration from the NT4 server to Samba Version 3 (Samba-3), you must also validate the security descriptors in the profiles share and network logon scripts.

In the migration scenario presented in this chapter, we use the following software components:

- Linux operating system
- Samba-3
- Lightweight Directory Access Protocol (LDAP)

The important key about accounts database migration is that the Samba-3 server will work with **`passdb backend`**, based on LDAP. **`ldapsam`** is a good option because an LDAP backend can be distributed for use with Backup Domain Controllers (BDCs) generally used for larger networks.

The example in this paper shows you how to migrate users, groups, and machine accounts from the Primary Domain Controller (PDC) Windows NT4-based environment to a single Samba-3 LDAP back-end database running on @server i5. The migration process includes data replication for a Windows NT4 registry-based accounts database, which resides in a Security Account Manager (SAM) to LDAP database.

The merging of multiple NT4 domains into one Samba-3 LDAP database can add significant value, considering the maximum utilization of @server i5 virtualization technology. This is especially true when compared with the alternative of migrating the same environment to Windows Server 200x and Active Directory.

You can also consolidate a lot of other workloads or services onto Linux on @server i5, besides the primary domain, file, and print server workloads covered in this chapter. The integration of user information on the LDAP database can provide additional side benefits other than simple migration. For example, this database can consolidate authentication for different applications, such as e-mail applications.

1.2 Scenario description

The objective of this scenario is to migrate user, group, and machine accounts from several NT4 domains into a single Samba-3 LDAP back-end database running on @server i5. The key objective of this scenario is to make the migration from Windows NT4 to Samba-3 Domain Control as easy as possible.

1.2.1 Benefits of running the workloads in Linux on eServer i5

Before you attempt migration to a Samba-3 on @server i5 controlled network, gain commitment to the change from all concerned parties. You must be able to explain precisely *why* the change is important for the organization and convince management and others on the following benefits:

- Improved disk manageability
- Improved security manageability
- Improved network manageability
- Better user level functionality

- Global availability of support with no strings attached
- Reduction of network operating costs
- Greater stability, reliability, performance, and availability
- Reduction of exposure caused by Microsoft withdrawal of NT4 support
- Avoidance of Microsoft license costs
- Reduction of the organization's dependency on Microsoft
- Lower cost of ownership
- Dynamic Server Message Block (SMB) servers (run more than one SMB/CIFS server per UNIX or Linux system)
- Creation of on-the-fly logon scripts
- Creation of on-the-fly policy files
- Manageability via an ssh connection
- Ability to implement a single signon architecture
- Ability to distribute authentication systems for absolute minimum wide area network bandwidth demand

In addition to the numerous benefits of using Linux itself, running the Linux server on @server i5 offers exceptional benefits. For example, you can have multiple Linux servers on a single @server i5. With multiple Linux logical partitions (LPARs) running in the same @server i5, you can have different networking services provided by different Linux partitions. All these partitions can benefit from IBM Virtualization Engine™ technology. This means that all these Linux partitions can work with the disk subsytems and network I/O being made available by i5/OS.

By *not* migrating your company's Windows NT4 domains to a Samba-3 on @server i5 controlled network, your company will see higher costs in operations due to:

- Maintenance of an infrastructure with a number of different physical servers, peripheral, and networking hardware results
- Increased electricity, air conditioning, and space requirements to house the additional machines

1.2.2 Understanding the migration details

Typical core networking services provided by Windows NT4 servers in a common Windows NT4 domain-based network include:

- Authentication services
- File services
- Print services
- Database services
- Web services
- Messaging services
- Infrastructure services such as Domain Name Service (DNS) and Dynamic Host Configuration Protocol (DHCP) services

Implementation details

Although we can migrate all of these services to run in a Linux server on @server i5, our focus in this scenario is to migrate the Windows NT4 domain to Samba services on Linux on @server i5.

Figure 1-1 shows a view of the environment before the migration.

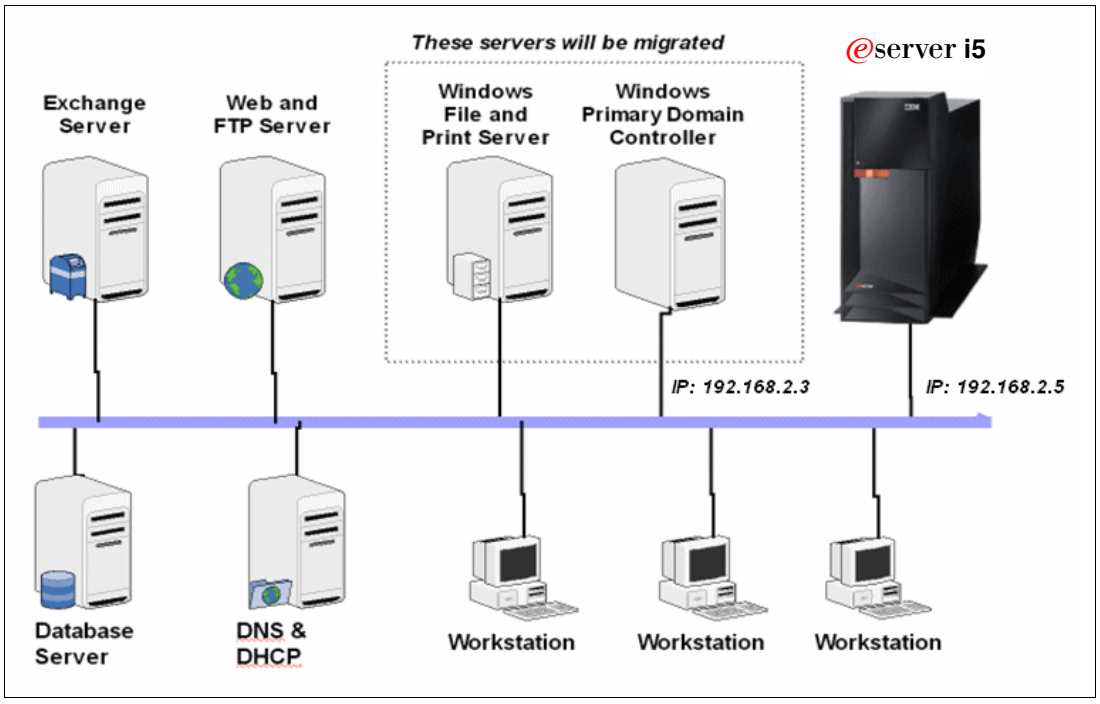


Figure 1-1 Environment view before the migration of Windows NT to Linux

Figure 1-2 shows a view of the environment after the migration. By comparing these two figures, you see that we migrate both PDC and file and print serving workloads from Windows NT to the Linux server running on @server i5.

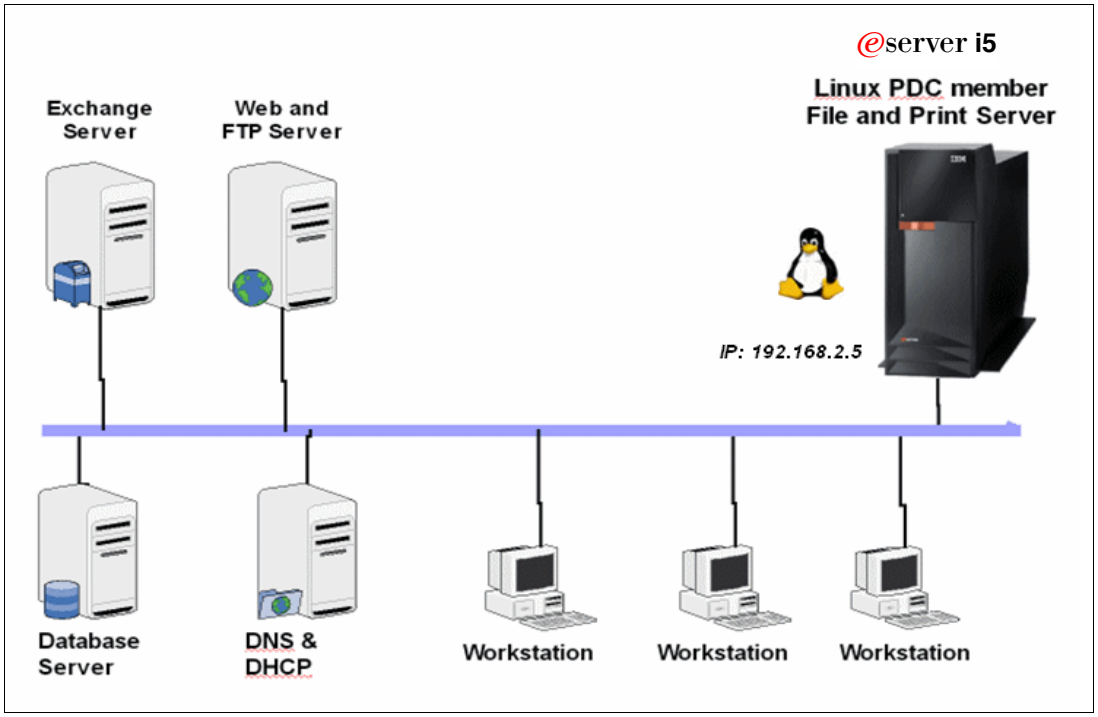


Figure 1-2 Environment view after migration of Windows NT to Linux

Our scenario entails the following details:

- All the machines, including Linux partition, are in the same subnet 192.168.2.0/24.
- The Windows NT4 server is used as a PDC and will be deactivated during the migration.
- The Linux distribution used is SUSE LINUX Enterprise Server 9 (SLES9) for @server i5.

> **Note:** The examples of the commands and configuration files shown in this chapter are based on SLES9. Therefore, the actual commands and configuration files in your particular implementation might be different depending on the distribution or version you use. However, conceptually, they should be the same.

- The name of the Windows NT domain is ITSOSMB.
- The NetBIOS name of the NT4 PDC is ITSONT4 (IP address 192.168.2.3).
- The Linux host name is *linux* (IP address 192.168.2.5).
- The Linux partition has a physical network interface setup that uses the previously listed IP address. The interface identifier is eth0.

Installation checklist

Prior to this type of migration, you must ensure that the following items are either installed or operational:

- The Windows NT4 style domain called ITSOSMB is operational.
- The Windows clients are already members of the domain.
- The Linux operating system is installed and operational.
- Samba-3 is installed with the necessary packages (see “Preparing the target Samba-3 server” on page 6). To check the Samba packages, run the following command:

  ```
  rpm -qa | grep samba
  ```

- Ensure that OpenLDAP is installed. To check, run the following command:

  ```
  rpm -qa | grep ldap
  ```

- All machines can resolve each other’s names using Windows Internetworking Name Services (WINS). We used the PDC to act as the WINS server for this scenario.

  You can test the name resolution by running the **`aping`** command on the host name.

1.3 Planning for migration

Essentially, the migration from Windows NT4 to Samba-3 involves the following aspects:

- Migration of data

  This migration can happen using different techniques. If you have a good network environment, for example that uses Gigabit Ethernet, you can share a storage area in the Samba server and copy it via the network. Otherwise, you can use backup media, such as tape or CD/DVD.

- Migration of a network environment

  You need to analyze which resources you use in your network environment before migration and implement the same resources in the Linux environment. For example, the user profile in PDC can load a BAT file in a local PDC disk area. You need to copy this script for Linux before the migration occurs.

- Users, groups, and machine accounts migration

  You need to import users, groups and machine accounts from PDC to the LDAP database.

Preparing the PDC stand-alone server to be migrated

Clean the PDC database by removing users, groups, or machines that do not need to exist in your network anymore.

Preparing the target Samba-3 server

Install the Samba-3 and LDAP packages in your Linux on @server i5. You can use the RPM command:

```
rpm -ivh package_name
```

Or you can use the YAST tool if you are using SLES9.

The migration scenario presented in this chapter uses the following packages:

- samba-3
- samba-winbind-3
- samba-client-3
- samba-doc-3
- openldap
- openldap2-client
- openldap2-back-perl
- perl-ldap
- perl-ldap-ssl
- nss_ldap
- pam_ldap
- ldapcpplib

Domain layout

You must pay particular attention to the location of the PDC and BDCs. For this scenario, we are working with LDAP authentication on the back end. The same database can be used by several different domains. In a complex organization, there can be a single LDAP database, which itself can be distributed (a master server and multiple subordinate (slave) servers) and simultaneously serve multiple domains.

From a design perspective, the number of users per server and the number of servers per domain should be scaled. In doing so, take into consideration the server capacity and network bandwidth.

A physical network segment may house several domains. Each domain may span multiple network segments. Where domains span routed network segments, consider and test the performance implications of the design and layout of a network.

Server share and directory layout

When it comes to designing an efficient network, the most important rule is to keep it simple. Every part of the infrastructure must be managed. The more complex it is, the greater the demand is to keep systems secure and functional.

Keep in mind the nature of how data must be shared. Carefully consider the layout of the physical disk space. Some data must be backed up. The simpler the disk layout is, the easier it will be to keep track of backup needs. Identify which backup media will meet your needs. For example, consider backup to tape, CD-ROM or DVD-ROM, or other offline storage medium. Plan and implement for minimum maintenance.

Keep your design and implementation simple, and document your design extensively. Have others audit your documentation. Do not create a complex mess that your successor will not understand.

Logon scripts

Logon scripts help to ensure that users gain the share and printer connections they need. The preferred controls should be affected throughout the group membership so that group information can be used to create a custom logon script using the `root preexec` parameters to the NETLOGON share.

1.4 Step-by-step migration guide

This section takes you step-by-step through the migration tasks for our scenario.

1.4.1 Task 1: Configuring OpenLDAP

To begin, you must configure OpenLDAP as explained in the following steps.

1. Configure the /etc/openldap/slapd.conf file. For this scenario, we use the file shown in Example 1-1, and make the changes as highlighted in bold.

Example 1-1 Contents of the /etc/openldap/slapd.conf file

```
#
# See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.
#
include etc/openldap/schema/core.schema
include etc/openldap/schema/cosine.schema
include etc/openldap/schema/inetorgperson.schema
include etc/openldap/schema/nis.schema
include etc/openldap/schema/samba3.schema

pidfile /var/run/slapd/slapd.pid
argsfile /var/run/slapd/slapd.args

database ldbm
directory /var/lib/ldap
suffix "dc=redbook,dc=net"
rootdn "cn=Manager,dc=redbook,dc=net"
rootpw manager
index objectClass,uidNumber,gidNumber eq
index member,mail eq,pres
index cn,displayname,uid,sn,givenname sub,eq,pres
index memberUID,sambaSID,sambaPrimaryGroupSID,sambaDomainName eq
index default sub

access to attr=userPassword,sambaLMPassword,sambaNTPassword
        by self write
        by * auth

access to *
        by * read
```

We make the following entries in this file as highlighted in Example 1-1.

- `database ldbm`

  This entry marks the beginning of a new database instance definition. Possible entries include bdb, dnssrv, ldap, ldbm, meta, monitor, null, passwd, perl, shell, sql, or tcl, depending on which back-end job serves the database.

– `directory /var/lib/ldap`

  This entry is the path of the database directory.

– `suffix "dc=redbook,dc=net"`

  This entry specifies the suffix of the queries that are passed to the back-end database. Multiple suffix lines can be given, and at least one is required for each database definition.

– `rootdn "cn=Manager,dc=redbook,dc=net"`

  This entry specifies the distinguished name (dn) that is not subject to access control or administrative limit restrictions for operations on this database.

– `rootpw manager`

  This entry specifies a password (or hash of the password) for the rootdn.

Note: The LDAP configuration information that is presented here is for demonstration purposes only.

2. Edit the /etc/openldap/ldap.conf file to include the contents as shown in bold in Example 1-2.

Example 1-2 Contents of the /etc/openldap/ldap.conf file

```
#
# LDAP Defaults
#

# See ldap.conf(5) for details
# This file should be world readable but not world writable.

BASE dc=redbook,dc=net
HOST 127.0.0.1
```

We make the following entries as highlighted in Example 1-2.

– `BASE dc=redbook,dc=net`

  This entry specifies the default base DN to use when performing LDAP operations.

– `HOST 127.0.0.1`

  This entry indicates where the LDAP database is located.

3. Edit the /etc/ldap.conf to include the contents as shown in Example 1-3.

Example 1-3 Contents of the /etc/ldap.conf file

```
#
# This is the configuration file for the LDAP nameservice
# switch library, the LDAP PAM module and the shadow package.
#

# Your LDAP server. Must be resolvable without using LDAP.
host 127.0.0.1

# The distinguished name of the search base.
base dc=redbook,dc=net


# The LDAP version to use (defaults to 3
# if supported by client library)
```

```
ldap_version 3

# The distinguished name to bind to the server with.
# Optional: default is to bind anonymously.

binddn cn=Manager,dc=redbook,dc=net

# The credentials to bind with.
# Optional: default is no credential.

bindpw manager

rootbinddn cn=Manager,dc=redbook,dc=net

# Use the OpenLDAP password change
# extended operation to update the password.

pam_password exop

nss_base_passwd ou=People,dc=redbook,dc=net?one
nss_base_shadow ou=People,dc=redbook,dc=net?one
nss_base_group ou=Groups,dc=redbook,dc=net?one

ssl no
```

We make the following entries to the file as highlighted in Example 1-3.

- `binddn cn=Manager,dc=redbook,dc=net`

  This entry specifies the default bind DN to use when performing LDAP operations.

- `bindpw manager`

  This directive sets the password for access control list (ACL) checking in conjunction with the "binddn" directive.

- `rootbinddn cn=Manager,dc=redbook,dc=net`

  This entry allows the manager user to change the password of the users.

- `nss_base_passwd ou=People,dc=redbook,dc=net?one`

  This entry helps to find users in the LDAP structure.

- `nss_base_shadow ou=People,dc=redbook,dc=net?one`

  This entry helps to find passwords in the LDAP structure.

- `nss_base_group ou=Groups,dc=redbook,dc=net?one`

  This entry helps to find groups in the LDAP structure.

4. Create an /etc/ldap.secret file and type the password that will be used to bind to the LDAP database when the effective user ID is root. In this scenario, we use a simple password “manager” for this purpose. If you edit the file directly, make sure that the file only has the password and not the double quotation marks. Make it readable only by root using the command:

```
linux:# echo "manager" >/etc/ldap.secret
linux:# chmod 600 /etc/ldap.secret
```

1.4.2 Task 2: Configuring the name service switch and starting LDAP

Complete the following steps:

1. Configure the name service switch (NSS) to identity management using LDAP. Edit the /etc/nsswitch.conf file to have the contents as shown in Example 1-4. The NSS configuration file is /etc/nsswitch.conf. Configuration in this file provides control for the user and group name resolutions to be done using different sources.

Example 1-4 Contents of the etc/nsswitch.conf file

```
#
# /etc/nsswitch.conf
#

passwd: files ldap
shadow: files ldap
group: files ldap

hosts: files wins dns
networks: files dns

services: files
protocols: files
rpc: files
ethers: files
netmasks: files
netgroup: files
publickey: files

bootparams: files
automount: files nis
aliases: files
```

   In this file, we change the `windind` entry as highlighted in Example 1-4. The entry `ldap` indicates a new place to get information about the NSS.

2. Start the OpenLDAP server.

```
linux:# rcldap start
```

1.4.3 Task 3: Configuring Samba

Follow these steps to configure Samba.

1. Edit the /etc/samba/smb.conf to include the contents as shown in Example 1-5.

Example 1-5 /etc/samba/smb.conf example

```
# smb.conf is the main Samba configuration file. You find a full commented
# version at /usr/share/doc/packages/samba/examples/smb.conf.SUSE
# Date: 2004-07-01
[global]
   workgroup = ITSOSMB
   printing = cups
   printcap name = cups
   cups options = raw
   printer admin = @ntadmin, root, administrator
   username map = /etc/samba/smbusers
   map to guest = Bad User
   logon path = \\%L\profiles\.msprofile
   logon home = \\%L\%U\.9xprofile
```

```
   logon drive = P:
   netbios name = linux
   syslog = 0
   log level = 1
   max log size = 3000
   log file = /var/log/samba/log.%m
   name resolve order = wins bcast hosts
   add user script = /var/lib/samba/sbin/smbldap-useradd.pl -m '%u'
   delete user script = /var/lib/samba/sbin/smbldap-userdel.pl '%u'
   add group script = /var/lib/samba/sbin/smbldap-groupadd.pl -p '%g'
   delete group script = /var/lib/samba/sbin/smbldap-groupdel.pl '%g'
   add user to group script = /var/lib/samba/sbin/smbldap-groupmod.pl -m '%u' '%g'
   delete user from group script = /var/lib/samba/sbin/smbldap-groupmod.pl -x '%u' '%g'
   set primary group script = /var/lib/samba/sbin/smbldap-usermod.pl -g '%g' '%u'
   add machine script = /var/lib/samba/sbin/smbldap-useradd.pl -w '%u'
   os level = 20
   domain logons = yes
   domain master = no
   preferred master = yes
   passdb backend = ldapsam:ldap://127.0.0.1/
   encrypt passwords = yes
   ldap ssl = no
   ldap suffix = dc=redbook,dc=net
   ldap machine suffix = ou=People
   ldap user suffix = ou=People
   ldap group suffix = ou=Groups
   ldap passwd sync = yes
   ldap admin dn = cn=Manager,dc=redbook,dc=net
   idmap backend = ldap:ldap://127.0.0.1/
   idmap uid = 10000-20000
   idmap gid = 10000-20000

# we use next line to point to the WINS server which NT4 PDC is acting as in our scenario
#you must point it to your proper WINS server

   wins server = 192.168.2.3

# we use next line to point to the WINS services provided by Samba, we will comment the
#above statement and uncomment the next line when we are ready to start the Samba services
#as we will be using the WINS services provided by Samba. If you have WINS services from
#some other server then you don't need to uncomment the next line in future.
#  wins support = yes

   logon home = \\%L\%U
   logon drive = Z:
   logon path = \\%L\profiles\%U
[netlogon]
   comment = Netlogon Share for Network Logins
   path = /var/lib/samba/netlogn
   guest ok = yes
   locking = no
[homes]
   comment = Home Directories
   valid users = %S
   browseable = No
   read only = No
   inherit permissions = Yes
   create mask = 0664
   directory mask = 0775
```

```
[docs]
   comment = Document for Everybody to browse
   path = /usr/share/doc
   valid users = @"Domain Users"
   read only = yes
[profiles]
   comment = Network Profiles Service
   path = %H
   read only = No
   store dos attributes = Yes
   create mask = 0600
   directory mask = 0700
   browseable = no
[printers]
   comment = All Printers
   path = /var/tmp
   printable = Yes
   create mask = 0600
   browseable = No
[print$]
   comment = Printer Drivers
   path = /var/lib/samba/drivers
   write list = @ntadmin root
   force group = ntadmin
   create mask = 0664
   directory mask = 0775
```

In this step, we make the following entries as highlighted in Example 1-5.

- `workgroup = ITSOSMB`

  This entry is the domain name of which this server intends to be a member.

- `netbios name = linux`

  This entry indicates the NetBIOS name of this Samba server. If you do not include this information in the smb.conf file, Samba will use the same name as the machine host name.

- `domain master = no`

  At this stage, we configure Samba not to be a master domain. We will change its status later.

- `passdb backend = ldapsam:ldap://127.0.0.1/`

  This configuration indicates that we are working with LDAP back-end database that is located in localhost.

- `wins server = 192.168.2.3`

  This entry shows the IP address of the Windows server™ that you are using at the moment, which in this case, is the IP address before the migration.

2. Samba should be able to do queries and make updates to the LDAP database. Enter the following command to handle Samba's own authentication to LDAP:

```
linux: # smbpasswd -w manager
Setting stored password for "cn=Manager,dc=redbook,dc=net" in secrets.tdb
```

3. Configure the smbldap-tools. This set of scripts is useful in managing users and groups in conjunction with LDAP. smbldap-tools is included with Samba-3 package distribution. On SLES, it is located in the /usr/share/doc/packages/samba/examples/LDAP/smbldap-tools directory. The smbldap-tools must be configured to match the server's LDAP configuration.

a. Copy the scripts from the /usr/share/doc/packages/samba/examples /LDAP/smbldap-tools directory to /var/lib/samba/sbin as shown in the following example:

```
linux:~# mkdir -p /var/lib/samba/sbin
linux:~# chown root.root /var/lib/samba/sbin
linux:~# cd /usr/share/doc/packages/samba/examples/LDAP/smbldap-tools
linux:# cp *.pl *.pm /var/lib/samba/sbin
linux:~# chmod -R 755 /var/lib/samba/sbin
```

b. Compile the **mkntpwd** tool and then install it in the /var/lib/samba/sbin and /usr/local/sbin directories as shown here:

```
linux:~# cd /usr/share/doc/packages/samba/examples/LDAP/smbldap-tools/mkntpwd
linux:~# make
```

> **Note:** If you do not have a **make** command, you need to install the package named *make*. You can check for the command by typing:
>
> ```
> pm -qa | grep make
> ```

The **mkntpwd** tool should now be executable. Copy this tool to the /var/lib/samba/sbin directory.

```
linux:# cp mkntpwd /var/lib/samba/sbin
```

c. Edit the smbldap_conf.pm file in the /var/lib/samba/sbin directory. Place the SID of the NT4 PDC in this file, along with other parameters. To get the SID, type:

```
linux:/var/lib/samba/sbin # net rpc getsid -S ITSONT4 -W ITSOSMB
Storing SID S-1-5-21-276639665-668693614-1844936127 for Domain ITSOSMB in
secrets.tdb
```

Note the SID carefully because it is necessary to make communication between Samba and LDAP available. Edit the /var/lib/samba/sbin/smbldap_conf.pm file. It is not possible to show the entire file, so we show only the parameters that are relevant for our scenario (see Example 1-6). The other defaults should be valid.

Example 1-6 /usr/bin/perl

```
#!/usr/bin/perl
use strict;
package smbldap_conf;

# smbldap-tools.conf : Q & D configuration file for smbldap-tools

#  This code was developped by IDEALX (http://IDEALX.org/) and
#  contributors (their names can be found in the CONTRIBUTORS file).
#
#                 Copyright (C) 2001-2002 IDEALX

$UID_START = 1000;
$GID_START = 1000;

# Put the NT4 domain SID here (as obtained in step 5c in the implementation steps)
# to obtain this number do: "net rpc getsid -S ITSONT4 -W ITSOSMB"

$SID='S-1-5-21-276639665-668693614-1844936127';

# LDAP Configuration #

# Ex: $slaveLDAP = "127.0.0.1";
$slaveLDAP = "127.0.0.1";
```

```
$slavePort = "389";

# Master LDAP : needed for write operations
# Ex: $masterLDAP = "127.0.0.1";
$masterLDAP = "127.0.0.1";
$masterPort = "389";

# Use SSL for LDAP
# If set to "1", this option will use start_tls for connection
# (you should also used the port 389)
$ldapSSL = "0";

# LDAP Suffix
# Ex: $suffix = "dc=IDEALX,dc=ORG";
$suffix = "dc=redbook,dc=net";


# Where are stored Users
# Ex: $usersdn = "ou=Users,$suffix"; for ou=Users,dc=IDEALX,dc=ORG
$usersou = q(People);
$usersdn = "ou=$usersou,$suffix";

# Where are stored Computers
# Ex: $computersdn = "ou=Computers,$suffix"; for ou=Computers,dc=IDEALX,dc=ORG
$computersou = q(People);
$computersdn = "ou=$computersou,$suffix";

# Where are stored Groups
# Ex $groupsdn = "ou=Groups,$suffix"; for ou=Groups,dc=IDEALX,dc=ORG
$groupsou = q(Groups);
$groupsdn = "ou=$groupsou,$suffix";

# Default scope Used
$scope = "sub";

# Unix password encryption (CRYPT, MD5, SMD5, SSHA, SHA)
$hash_encrypt="MD5";

# Credential Configuration #

# Ex: $binddn = "cn=Manager,$suffix"; for cn=Manager,dc=IDEALX,dc=org
$binddn = "cn=Manager,$suffix";

# Bind DN passwd used
# Ex: $bindpasswd = 'secret'; for 'secret'
$bindpasswd = "manager";

# Unix Accounts Configuration #

# Default Login Shell
# Ex: $_userLoginShell = q(/bin/bash);
$_userLoginShell = q(/bin/bash);

# Home directory prefix (without username)
# Ex: $_userHomePrefix = q(/home/);
$_userHomePrefix = q(/home/);

# SAMBA Configuration #

$_userSmbHome = q(\\\\ITSONT4\\homes);
```

```
$_userProfile = q(\\\\ITSONT4\\profiles\\);

$_userHomeDrive = q(H:);

$with_smbpasswd = 0;
$smbpasswd = "/usr/bin/smbpasswd";
$mk_ntpasswd = "/var/lib/samba/sbin/mkntpwd";
```

We make the following entries as shown in Example 1-6.

- `$masterLDAP = "127.0.0.1";`

  This entry indicates that we are setting that LDAP server as the localhost.

- `$suffix = "dc=redbook,dc=net";`

  This entry specifies the DN suffix of queries that will be passed to this back-end database.

- `$hash_encrypt="MD5";`

  In this case, we are setting the cryptography based on the MD5 algorithm.

- `$binddn = "cn=Manager,$suffix";`

  This entry specifies the default bind DN to use when performing LDAP operations. The bind DN must be specified as a DN in the LDAP format.

- `$bindpasswd = "manager";`

  This entry indicates the password used for binddn (default bind DN).

- `$_userSmbHome = q(\\\\ITSONT4\\homes);`

  This entry is the location of user home directory.

- `$_userProfile = q(\\\\ITSONT4\\profiles\\);`

  This entry is the directory that will contain the user profiles.

- `$mk_ntpasswd = "/var/lib/samba/sbin/mkntpwd";`

  This entry shows the path of var/lib/samba/sbin/mkntpwd, which is responsible for user password authentication.

1.4.4 Task 4: Migrating the database

Use these steps to migrate the database.

1. Prepare the structure into a directory as shown in Example 1-7.

Example 1-7 /var/lib/samba/sbin example

```
linux:/var/lib/samba/sbin # ./smbldap-populate.pl
Using builtin directory structure
adding new entry: dc=redbook,dc=net
adding new entry: ou=People,dc=redbook,dc=net
adding new entry: ou=Groups,dc=redbook,dc=net
adding new entry: ou=People,dc=redbook,dc=net
adding new entry: uid=Administrator,ou=People,dc=redbook,dc=net
adding new entry: uid=nobody,ou=People,dc=redbook,dc=net
adding new entry: cn=Domain Admins,ou=Groups,dc=redbook,dc=net
adding new entry: cn=Domain Users,ou=Groups,dc=redbook,dc=net
adding new entry: cn=Domain Guests,ou=Groups,dc=redbook,dc=net
adding new entry: cn=Administrators,ou=Groups,dc=redbook,dc=net
adding new entry: cn=Users,ou=Groups,dc=redbook,dc=net
```

```
adding new entry: cn=Guests,ou=Groups,dc=redbook,dc=net
adding new entry: cn=Power Users,ou=Groups,dc=redbook,dc=net
adding new entry: cn=Account Operators,ou=Groups,dc=redbook,dc=net
adding new entry: cn=Server Operators,ou=Groups,dc=redbook,dc=net
adding new entry: cn=Print Operators,ou=Groups,dc=redbook,dc=net
adding new entry: cn=Backup Operators,ou=Groups,dc=redbook,dc=net
adding new entry: cn=Replicator,ou=Groups,dc=redbook,dc=net
adding new entry: cn=Domain Computers,ou=Groups,dc=redbook,dc=net
```

2. Restart OpenLDAP by entering the following command:

```
linux:~ # rcldap restart
```

3. Verify that the NSS resolver can interrogate the LDAP using the **getent** command as shown in the following example. The command shows the user content in /etc/passwd and in the LDAP database.

```
linux:~ # getent passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/bin/bash
....output snipped for better readability....
nobody:x:65534:65533:nobody:/var/lib/nobody:/bin/bash
+::0:0:::
Administrator:x:998:512:Netbios Domain Administrator:/home/:/bin/false
nobody:x:999:514:nobody:/dev/null:/bin/false
```

Also, verify the groups as shown in the following example. This verification includes the content in the /etc/group linux file and in the LDAP database, and indicates how it is specified in the /etc/nsswitch.conf file.

```
linux:~ # getent group
root:x:0:
bin:x:1:daemon
....output snipped for better readability...
Domain Admins:x:512:Administrator
Domain Users:x:513:
Domain Guests:x:514:
Administrators:x:544:
Users:x:545:
Guests:x:546:nobody
Power Users:x:547:
Account Operators:x:548:
Server Operators:x:549:
Print Operators:x:550:
Backup Operators:x:551:
Replicator:x:552:
Domain Computers:x:553:
```

4. Locate the administrator's ID by using the **getent** command.

```
linux: # getent passwd | grep Administrator
Administrator:x:998:512:Netbios Domain Administrator:/home/:/bin/false
```

Change the administrator's UID to 0 by using the **smbldap-tools** script.

```
linux:/var/lib/samba/sbin # ./smbldap-usermod.pl -u 0 Administrator
```

Confirm the change by typing:

```
linux:/var/lib/samba/sbin # getent passwd | grep Administrator
Administrator:x:0:512:Netbios Domain Administrator:/home/:/bin/false
```

5. Verify that Samba can see all of the Windows Domain Group mappings.

```
linux: # net groupmap list
Domain Admins (S-1-5-21-276639665-668693614-1844936127-512) -> Domain Admins
Domain Users (S-1-5-21-276639665-668693614-1844936127-513) -> Domain Users
Domain Guests (S-1-5-21-276639665-668693614-1844936127-514) -> Domain Guests
Administrators (S-1-5-21-276639665-668693614-1844936127-544) -> Administrators
users (S-1-5-21-276639665-668693614-1844936127-545) -> Users
Guests (S-1-5-21-276639665-668693614-1844936127-546) -> Guests
Power Users (S-1-5-21-276639665-668693614-1844936127-547) -> Power Users
Account Operators (S-1-5-21-276639665-668693614-1844936127-548) -> Account Operators
Server Operators (S-1-5-21-276639665-668693614-1844936127-549) -> Server Operators
Print Operators (S-1-5-21-276639665-668693614-1844936127-550) -> Print Operators
Backup Operators (S-1-5-21-276639665-668693614-1844936127-551) -> Backup Operators
Replicator (S-1-5-21-276639665-668693614-1844936127-552) -> Replicator
Domain Computers (S-1-5-21-276639665-668693614-1844936127-553) -> Domain Computers
```

6. Samba is ready to join the Windows NT4 domain as a BDC. You need to do this for the server to trust and import user, groups, and machine accounts.

```
linux: # net rpc join -U Administrator
Password:
Joined domain ITSOSMB.
```

   Type the Windows NT domain administrator's password when prompted. The Linux server must exist in the PDC.

7. Import the Windows NT SAM database to Samba using the vampire option of the **net** command.

```
linux: # net rpc vampire -S ITSONT4
Fetching DOMAIN database
SAM_DELTA_DOMAIN_INFO not handled
Creating account: Administrator
[2004/08/20 13:28:22, 0] passdb/pdb_ldap.c:ldapsam_add_sam_account(1573)
  ldapsam_add_sam_account: User 'Administrator' already in the base, with samba
attributes
Creating account: Guest
Creating account: IUSR_ITSONT4
Creating account: vaseem
Creating account: freddy
Creating account: stacey
Creating account: vaclav
Creating account: yessong
Creating account: user1
Creating account: hrd1
Creating account: TEST1$
Creating account: CRUZ$
Creating account: ANSARI$
Creating account: JOHNSON$
Creating account: MAT123$
Creating account: fin1
Creating account: operator
Creating account: rehan
Creating account: farah
Creating account: zeeshan
Creating account: shehzad
Creating account: ZUBEDA$
Creating account: NTWKS$
Creating account: rumaisa
Creating account: WINXP$
Creating account: WIN2K33$
Creating account: XPPROF$
```

```
Creating account: linux$
Group members of Domain Admins: yessong,vaclav,vaseem,
deleting user Administrator from group Domain Admins
adding user yessong to group Domain Admins
adding user vaclav to group Domain Admins
adding user vaseem to group Domain Admins
Group members of Domain Users:
Administrator,IUSR_ITSONT4(primary),rumaisa(primary),vaseem(primary),freddy(primary),sta
cey(primary),vaclav(primary),yessong(primary),user1(primary),user2(primary),user3(primar
y),user4(primary),operator(primary),hrd1(primary),TEST1$(primary),CRUZ$(primary),ANSARI$
(primary),JOHNSON$(primary),MAT123$(primary),TEST2$(primary),TEST3$(primary),fin1(primar
y),fin2(primary),fin3(primary),ZUBEDA$(primary),rehan(primary),farah(primary),zeeshan(pr
imary),shehzad(primary),NTWKS$(primary),WINXP$(primary),NTWKS11$(primary),NTWKS22$(prima
ry),WINXP11$(primary),WINXP22$(primary),WIN2K11$(primary),WIN2K22$(primary),WIN2K33$(pri
mary),XPPROF$(primary),linux$(primary),
deleting user Guest from group Domain Users
deleting user IUSR_ITSONT4 from group Domain Users
deleting user vaseem from group Domain Users
deleting user freddy from group Domain Users
...output snip....
Creating unix group: 'FINANCE'
Creating unix group: 'HRD'
Creating unix group: 'ITUsers'
Creating unix group: 'Project'
Fetching BUILTIN database
SAM_DELTA_DOMAIN_INFO not handled
[2004/08/20 13:28:52, 0] passdb/pdb_ldap.c:ldapsam_add_group_mapping_entry(2022)
  ldapsam_add_group_mapping_entry: Group 548 already exists in LDAP
[2004/08/20 13:28:52, 0] passdb/pdb_ldap.c:ldapsam_add_group_mapping_entry(2022)
  ldapsam_add_group_mapping_entry: Group 544 already exists in LDAP
[2004/08/20 13:28:52, 0] passdb/pdb_ldap.c:ldapsam_add_group_mapping_entry(2022)
  ldapsam_add_group_mapping_entry: Group 551 already exists in LDAP
```

Note: Do not be alarmed by the errors thrown by the vampire process. We do not show the rest of the output here.

8. The NT SAM database migration is completed, but the migration process is not. The administrator password was not migrated because the user existed in the LDAP database before importing it.

   Set the administrator password using **smbldap-tools**.

   ```
   linux:/var/lib/samba/sbin # ./smbldap-passwd.pl Administrator
   ```

   When prompted to enter the password, set the password to be same as the administrator's password in the NT domain.

9. We have now made a copy of information about the users, groups, and machines from the actual PDC to the LDAP database.

   Use the following command to check the contents of the information in LDAP:

   ```
   ldapsearch -x
   ```

1.4.5 Task 5: Migrating the domain controller

You now have the information about users, groups, and machines in the Microsoft PDC, running on a stand-alone server, and in LDAP, running on Linux with Samba-3 on @server i5. At this point, make sure that Samba is not running, because you need to set Samba to work as the domain controller. You can verify that Samba is not running by using the following command:

```
linux:~ # ps -ef | grep smb | grep -v grep
linux:~ #
```

Now follow these steps:

1. Prepare a Samba configuration to work as the domain controller. Edit the /etc/samba/smb.conf file as shown in by the highlighted areas in Example 1-8.

Example 1-8 smb.conf

```
# smb.conf is the main Samba configuration file. You find a full commented
# version at /usr/share/doc/packages/samba/examples/smb.conf.SUSE
# Date: 2004-07-01
[global]
   workgroup = ITSOSMB
   printing = cups
   printcap name = cups
   cups options = raw
   printer admin = @ntadmin, root, administrator
   username map = /etc/samba/smbusers
   map to guest = Bad User
   logon path = \\%L\profiles\.msprofile
   logon home = \\%L\%U\.9xprofile
   logon drive = P:
   netbios name = itsont4
   syslog = 0
   log level = 1
   max log size = 3000
   log file = /var/log/samba/log.%m
   name resolve order = wins bcast hosts
   add user script = /var/lib/samba/sbin/smbldap-useradd.pl -m '%u'
   delete user script = /var/lib/samba/sbin/smbldap-userdel.pl '%u'
   add group script = /var/lib/samba/sbin/smbldap-groupadd.pl -p '%g'
   delete group script = /var/lib/samba/sbin/smbldap-groupdel.pl '%g'
   add user to group script = /var/lib/samba/sbin/smbldap-groupmod.pl -m '%u' '%g'
   delete user from group script = /var/lib/samba/sbin/smbldap-groupmod.pl -x '%u' '%g'
   set primary group script = /var/lib/samba/sbin/smbldap-usermod.pl -g '%g' '%u'
   add machine script = /var/lib/samba/sbin/smbldap-useradd.pl -w '%u'
   os level = 99
   domain logons = yes
   domain master = yes
   preferred master = yes
   passdb backend = ldapsam:ldap://127.0.0.1/
   encrypt passwords = yes
   ldap ssl = no
   ldap suffix = dc=redbook,dc=net
   ldap machine suffix = ou=People
   ldap user suffix = ou=People
   ldap group suffix = ou=Groups
   ldap passwd sync = yes
   ldap admin dn = cn=Manager,dc=redbook,dc=net
   idmap backend = ldap:ldap://127.0.0.1/
   idmap uid = 10000-20000
   idmap gid = 10000-20000

# we use next line to point to the WINS server which NT4 PDC is acting as in our scenario
#you must point it to your proper WINS server

#  wins server = 192.168.2.3
```

```
# we use next line to point to the WINS services provided by Samba, we will comment the
#above statement and uncomment the next line when we are ready to start the Samba services
#as we will be using the WINS services provided by Samba. If you have WINS services from
#some other server then you don't need to uncomment the next line in future.
   wins support = yes

   logon home = \\%L\%U
   logon drive = Z:
   logon path = \\%L\profiles\%U
[netlogon]
   comment = Netlogon Share for Network Logins
   path = /var/lib/samba/netlogn
   guest ok = yes
   locking = no
[homes]
   comment = Home Directories
   valid users = %S
   browseable = No
   read only = No
   inherit permissions = Yes
   create mask = 0664
   directory mask = 0775

[docs]
   comment = Document for Everybody to browse
   path = /usr/share/doc
   valid users = @"Domain Users"
   read only = yes
[profiles]
   comment = Network Profiles Service
   path = %H
   read only = No
   store dos attributes = Yes
   create mask = 0600
   directory mask = 0700
   browseable = no
[printers]
   comment = All Printers
   path = /var/tmp
   printable = Yes
   create mask = 0600
   browseable = No
[print$]
   comment = Printer Drivers
   path = /var/lib/samba/drivers
   write list = @ntadmin root
   force group = ntadmin
   create mask = 0664
   directory mask = 0775
```

We make the following changes as highlighted in Example 1-8.

- `netbios name = itsont4`

  This entry is the same NetBIOS name of PDC.

- `os level = 99`

  The value of this parameter determines whether Samba has a chance of becoming a local master browser for the WORKGROUP in the local broadcast area.

- `domain master = yes`

  This value determines whether Samba is a primary domain in the network.

- `wins support = yes`

  This value determines whether Samba works as a Windows server.

Comment the line `wins server = 192.168.2.3` or delete it. Samba is now for ready for Wins service.

The NetBIOS name change will handle the profile path issues since the migrated data still points to the Windows NT PDC's NetBIOS name. Changing the NetBIOS name of the Samba server to that of the Windows NT PDC will resolve this issue.

2. Shut down the Windows NT PDC.
3. The Samba server is now ready to take the role of the PDC. Start the Samba services in the order shown:

```
linux:~# rcnmb start
linux:~# rcsmb start
```

4. Make the services autorun whenever the Linux partition boots or restarts.

```
#linux:~# chkconfig ldap on
#linux:~# chkconfig nmb on
#linux:~# chkconfig smb on
```

This concludes the migration process. We have eliminated a Windows domain controller from the network.

Note: This sequence of steps was used for minimal downtime for users in the network. We prepared an entirely new environment to make a single shutdown in an old PDC and a startup of the new domain controller running on @server i5.

1.5 Facilities to administrate LDAP after migration

You can administrate LDAP using a command line. However the same tools are available for you to do administration via a graphical interface. This section presents an example of using phpLDAPadmin, one of the most popular tools for administration.

1.5.1 Installing phpLDAPadmin

Follow these steps:

1. Install the following packages and their dependencies:
   - php4
   - php4-pear
   - php4-ldap
   - apache2
   - apache2-mod_php4
2. Start a download from phpLDAPadmin. Point your browser to:

   http://phpldapadmin.sourceforge.net/

   We downloaded the file phpldapadmin-0.9.5.tar.gz. Place the file in the Linux server in the /Redbook directory.

3. Uncompress the file.

```
cd /Redbook
tar -xzvf phpldapadmin-0.9.5.tar.gz
```

1.5.2 Configuring phpLDAPadmin

Now complete these steps:

1. Edit the file named /Redbook/phpldapadmin-0.9.5/config.php as shown in Example 1-9.

Example 1-9 phpldapadmin

```
<?php

$blowfish_secret = '';

$i=0;
$servers = array();
$servers[$i]['name'] = 'Yessong Redbooks';
$servers[$i]['host'] = 'localhost';
$servers[$i]['base'] = 'dc=redbook,dc=net';
$servers[$i]['port'] = 389;
$servers[$i]['auth_type'] = 'config';
$servers[$i]['login_dn'] = 'cn=Manager,dc=redbook,dc=net';
$servers[$i]['login_pass'] = 'manager';
$servers[$i]['tls'] = false;
$servers[$i]['low_bandwidth'] = false;
$servers[$i]['default_hash'] = 'crypt';
$servers[$i]['login_attr'] = 'dn';
$servers[$i]['login_string'] = 'uid=<username>';
$servers[$i]['login_class'] = '';
$servers[$i]['read_only'] = false;
$servers[$i]['show_create'] = true;
$servers[$i]['enable_auto_uid_numbers'] = false;
$servers[$i]['auto_uid_number_mechanism'] = 'search';
$servers[$i]['auto_uid_number_search_base'] = 'ou=People,dc=example,dc=com';
$servers[$i]['auto_uid_number_min'] = 1000;
$servers[$i]['auto_uid_number_uid_pool_dn'] = 'cn=uidPool,dc=example,dc=com';
$servers[$i]['auto_uid_number_search_dn'] = '';
$servers[$i]['auto_uid_number_search_dn_pass'] = '';
$servers[$i]['disable_anon_bind'] = false;
$servers[$i]['custom_pages_prefix'] = 'custom_';
$servers[$i]['unique_attrs_dn'] = '';
$servers[$i]['unique_attrs_dn_pass'] = '';
$jpeg_temp_dir = "/tmp";
$hide_configuration_management = false;
$tree_display_format = '%rdn';
$search_deref = LDAP_DEREF_ALWAYS;
$tree_deref = LDAP_DEREF_NEVER;
$export_deref = LDAP_DEREF_NEVER;
$view_deref = LDAP_DEREF_NEVER;
$language = 'auto';
$enable_mass_delete = false;
$anonymous_bind_implies_read_only = true;
$anonymous_bind_redirect_no_tree = false;
$cookie_time = 0; // seconds
$tree_width = 320; // pixels
$jpeg_tmp_keep_time = 120; // seconds
$show_hints = true; // set to false to disable hints
$search_result_size_limit = 50;
```

```
$default_search_display = 'list';
$obfuscate_password_display = false;
$search_attributes = "uid, cn, gidNumber, objectClass, telephoneNumber, mail, street";
$search_attributes_display = "User Name, Common Name, Group ID, Object Class, Phone Number,
Email, Address";
$search_result_attributes = "cn, sn, uid, postalAddress, telephoneNumber";
$search_criteria_options = array( "equals", "starts with", "contains", "ends with", "sounds
like" );
$multi_line_attributes = array( "postalAddress", "homePostalAddress", "personalSignature"
);
$multi_line_syntax_oids = array(
                            "1.3.6.1.4.1.1466.115.121.1.40",
                            "1.3.6.1.4.1.1466.115.121.1.41"  );
$friendly_attrs = array();
$friendly_attrs[ 'facsimileTelephoneNumber' ] =         'Fax';
$friendly_attrs[ 'telephoneNumber' ]  =                 'Phone';
$q=0;
$queries = array();
$queries[$q]['name'] = 'Samba Users';       /* The name that will appear in the simple
search form */
$queries[$q]['server'] = '0';               /* The ldap server to query, must be defined in
the $servers list above */
$queries[$q]['base'] = 'dc=redbook,dc=net'; /* The base to search on */
$queries[$q]['scope'] = 'sub';              /* The search scope (sub, base, one) */
$queries[$q]['filter'] =
'(&(|(objectClass=sambaAccount)(objectClass=sambaSamAccount))(objectClass=posixAccount)(!(u
id=*$)))';
$queries[$q]['attributes'] = 'uid, smbHome, uidNumber';
$q++;
$queries[$q]['name'] = 'Samba Computers';
$queries[$q]['server'] = '0';
$queries[$q]['base'] = 'dc=redbook,dc=net';
$queries[$q]['scope'] = 'sub';
$queries[$q]['filter'] = '(&(objectClass=sambaAccount)(uid=*$))';
$queries[$q]['attributes'] = 'uid, homeDirectory';


?>
```

We make the following changes as highlighted in Example 1-9.

- `$servers[$i]['name] = ''Yessong Redbooks';`

  This is a convenient name that will appear in the tree viewer and throughout phpLDAPadmin to identify this LDAP server to users.

- `$servers[$i]['base'] = 'dc=redbook,dc=net';`

  This entry indicates the base DN of the LDAP server.

- `$servers[$i]['login_dn'] = 'cn=Manager,dc=redbook,dc=net';`

  This entry is the DN of the user for phpLDAPadmin to bind with.

- `$servers[$i]['login_pass'] = 'manager';`

  This entry indicates the LDAP password.

- `$queries[$q]['base'] = 'dc=redbook,dc=net';`

  This entry defines again the base DN of the LDAP server.

2. Configure Apache by changing the lines in the /etc/apache2/default-server.conf file, with comments as shown in Example 1-10.

Example 1-10 /etc/apache2/default-server.conf example

```
#DocumentRoot "/srv/www/htdocs"
DocumentRoot "/Redbook/phpldapadmin-0.9.5/"
#<Directory "/srv/www/htdocs">
<Directory "/Redbook/phpldapadmin-0.9.5/">
```

Note: The example of Apache shown here includes only the basic settings without security configuration. To learn more about the Apache configuration, see the documentation located on the Web at:

`http://www.apache.org`

1.5.3 Starting phpLDAPadmin

Use these step to start phpLDAPadmin.

1. Start Apache2.

   ```
   rcapache2 start
   ```

2. Check the phpLDAPadmin using a browser connected in same network as shown in Figure 1-3.

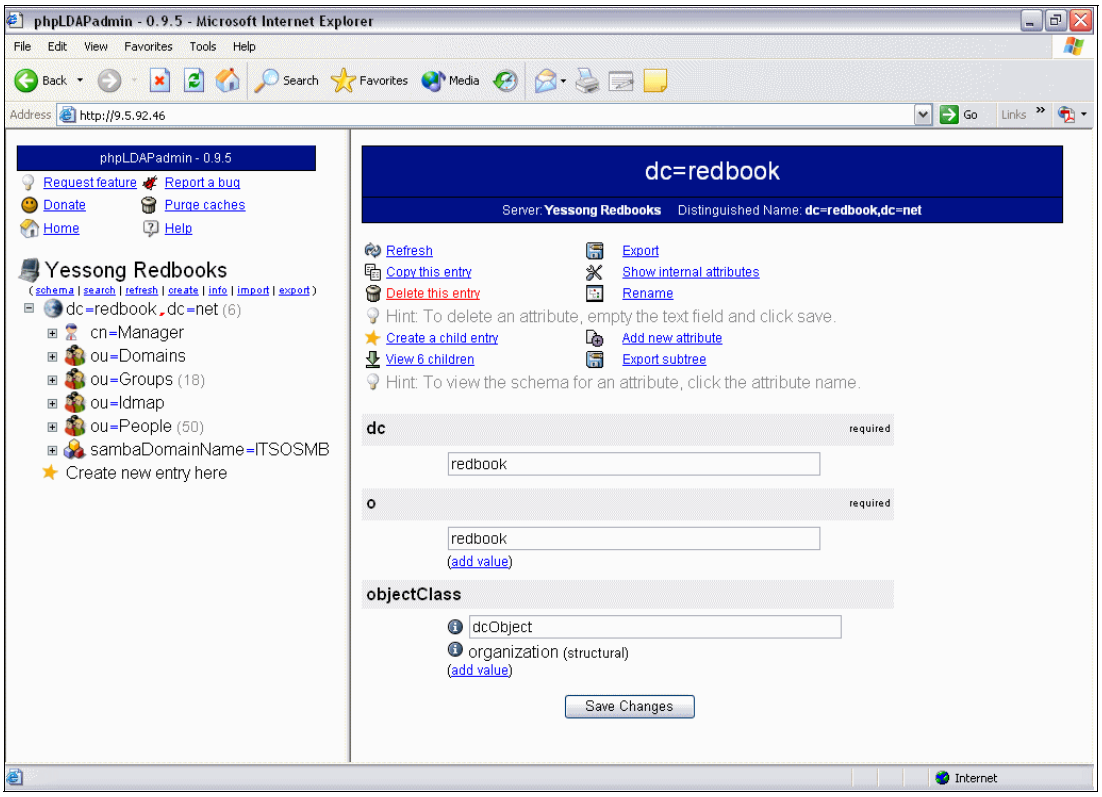


Figure 1-3 phpLDAPadmin using a browser

To learn more about phpLDAPadmin, go to:

`http://phpldapadmin.sourceforge.net`

2

Migrating a Windows PDC member to Linux PDC member on eServer i5

This chapter presents an overview of how to migrate your Microsoft file and print server Primary Domain Controller (PDC) member to a Linux Samba Version 3 (Samba-3)-based PDC member on @server i5. With this solution, you can migrate one or more file or print servers on your network, working as a PDC member, to Linux with Samba on @server i5, without making changes in your domain controller environment.

To keep the stand-alone server in your network, use the information in this paper to add a new Samba-3 file server based on @server i5 as a domain member server. In doing so, you set up the Samba server to become a member of the Windows NT 4.0-based PDC. When a client accesses shares on the Samba domain member server, Samba passes off the authentication to the domain controller rather than performing the task on the local system.

For Windows workstations and servers to participate in domain security, you need to make them domain members. Samba-3 can join the Windows NT4-style domain as a native member server or a Samba domain control network. Domain membership has many advantages:

- Windows workstation users gain the benefit of single signon (SSO).
- Domain user access rights and file ownership and access controls can be set from the single domain Security Account Manager (SAM) database (works with domain member servers and with Windows workstations that are domain members).
- Only Windows NT4, 200x, and XP Professional workstations that are domain members can use the network logon facilities.
- Domain member workstations can be better controlled through the use of policy files (NTConfig.POL) and desktop profiles.
- Through the use of logon scripts, users can be given transparent access to network applications that run off the application servers.

2.1 Understanding the terminology

A *machine trust account* is an account that is used to authenticate a client machine to the domain controller server. In Windows terminology, this is known as a *computer account*. The purpose of the machine trust account is to prevent a rogue user and domain controller from colliding to gain access to a domain member workstation.

The machine trust account's password acts as the shared secret for secure communication with the domain controller. This is a security feature to prevent an unauthorized machine, with the same NetBIOS name, from joining the domain and being permitted access to domain user and group accounts. Windows NT, 200x and XP Professional clients use machine trust accounts, but Windows 9x, Me, and XP Home clients do not. Therefore, a Windows 9x, Me, and XP Home client is never a true member of a domain because it does not possess a machine trust account, nor does it have a shared secret with the domain controller.

There are three ways to create machine trust accounts.

- Manual creation from the UNIX or Linux command line

  Here, both the Samba and corresponding UNIX account are created manually.

- Using the Windows NT4 Server Manager, either from an NT4 domain member server, or using the Nexus toolkit available from the Microsoft Web site

  This tool can be run from any Windows machine as long as the user is logged on as the administrator account.

- On-the-fly creation

  The Samba machine trust account is automatically created by Samba at the time the client is joined to the domain. For security, we recommend that you use this method. The corresponding UNIX account may be created automatically or manually.

2.2 Scenario description

The objective of this chapter's migration scenario is to migrate Windows-based file and print servers to Linux Samba without making changes in the current implementation of the domain controller.

2.2.1 Scenario view before integration

Figure 2-1 illustrates the file and print serving network before the migration. In addition to file and print servers which are Windows based, Windows NT is the PDC, which is used for authentication purposes.

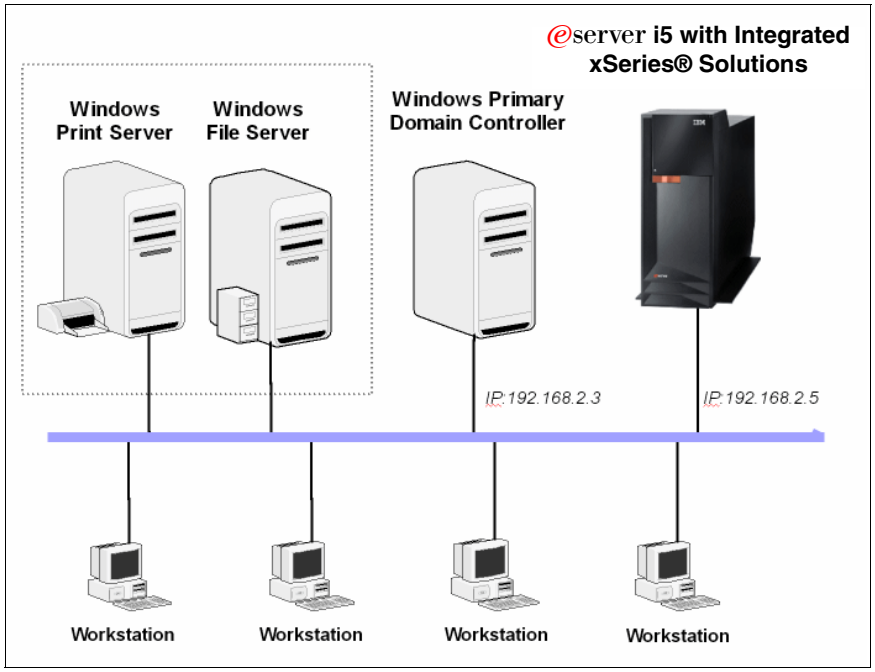


Figure 2-1 Environment view before migration of a Windows PDC member to a Linux PDC member

2.2.2 Scenario view after integration

A Samba server, when integrated in a Windows NT4 style domain network, can be configured to provide file and print services. Therefore, the Windows servers which were providing these services become eliminated. The Samba server is installed and configured on Linux installed on the @server i5 server as illustrated in Figure 2-2.

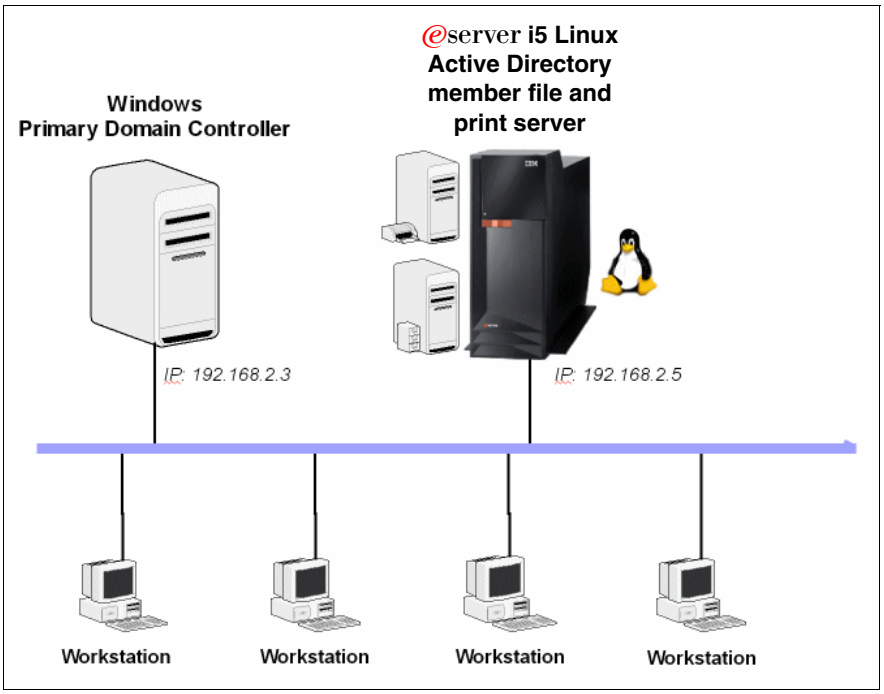


Figure 2-2 Environment view after migration of a Windows PDC member to a Linux PDC member

2.2.3 Network information of the scenario

The following list highlights information about the network used in the scenario as presented in this chapter.

- All the machines, including @server i5 with a Linux partition, are in the same subnet 192.168.2.5/24.
- Windows NT4 Server is used as a PDC.
- The Linux distribution used SUSE Linux Enterprise Server 9 (SLES9) for @server i5, with Samba-3 installed.
- The name of the Windows NT domain is ITSOSMB.
- The host name that will be used on the Linux Samba server on @server i5 is rchas10s (192.168.2.5).
- The NetBIOS name of the Linux Samba server is linuxOni5.
- The domain's PDC NetBIOS name is ITSONT4 (192.168.2.3).

If the server that you intend to migrate is a file server, plan the best choice to make a copy of files from Windows to Linux Samba on @server i5. Usually, copies are made using network or backup media. In addition, you must migrate your printers to the Samba server using the /etc/samba/smb.conf file.

2.3 Step-by-step migration guide

This section presents essential information to help you implement configure the name service switch (NSS) and Samba server on @server i5.

In this migration, you must configure the following two files on Linux:

- NSS configuration file /etc/nsswitch.conf
- Samba configuration file /etc/samba/smb.conf

2.3.1 Name service switch configuration file

The operating system uses several databases of information about hosts, ipnodes, users (passwd and shadow), and groups. The data can come from a variety of sources. For example, you can find host names and host addresses in /etc/hosts, NIS, NIS+, LDAP, or Domain Name System (DNS). Zero or more sources may be used for each database. The sources and their lookup order are specified in the /etc/nsswitch.conf file.

Note: You have to make some changes in the /etc/nsswitch.conf file. These changes include adding the `winbind` value to the “passwd” and “group” keywords.

The highlighted information in Example 2-1 shows where in the /etc/nsswitch/conf file to configure it to search in the winbind service.

Example 2-1 The /etc/nsswitch/conf file changed to search in the winbind service

```
# /etc/nsswitch.conf
#
# An example Name Service Switch config file
passwd: files winbind
group: files winbind
hosts: files dns wins
networks: files dns
services: files
protocols: files
rpc: files
ethers:files
netmasks: files
netgroup: files
publickey:files
bootparams: files
automount: files
aliases: files
```

Note: Winbindd is used to resolve user and group information from a Windows NT server.

2.3.2 Samba configuration file

Samba is fully configurable, and all configurations are made in the /etc/samba/smb.conf file. The parameters set in this file determine the behavior of the Samba service and the services that this server provides to your network. Example 2-2 shows how to configure this file for the scenario.

Example 2-2 The etc/samba/smb.conf file

```
# smb.conf is the main Samba configuration file. You find a full commented
# version at /usr/share/doc/packages/samba/examples/smb.conf.SUSE if the
# samba-doc package is installed.
#
# File          :/etc/samba/smb.conf
# Objective     :This file was configured to
#                Redbook IS-4753-R01 by residents
# Date          :2005-02-02
#

[global]
        workgroup = ITSOSMB
        netbios name = LinuxOni5
        security = domain
        server string = Samba on eServer i5
        os level = 10
        wins server = 192.168.2.3
        name resolve order = wins bcast hosts
        username map = /etc/samba/smbusers
        interfaces = eth0, lo
        bind interfaces only = yes
        log level = 1
        log file = /var/log/samba/%m
        max log size = 1024
        idmap uid = 10000-20000
        idmap gid = 10000-20000
        template primary group = "Domain Users"
        template shell = /bin/bash
        winbind separator = +
        printing = cups
        printcap name = cups
        printer admin = root
        socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
        unix charset = LOCALE

[Docs]
        comment = Docs for everybody
        path  = /usr/share/doc
        public = yes
        guest ok = yes

[homes]
        comment = Home Directories
        path = /livio
        browseable = yes
        read only = no
        store dos attributes = Yes
        create mask = 0600
        directory mask = 0700
```

```
[printers]
        comment = Samba printer Spool
        path = /var/spool/samba
        printable = Yes
        create mask = 0600
        browseable = No
        guest ok = yes

[print$]
        comment = Printer Drivers
        path = /var/lib/samba/drivers
        #write list = @ntadmin root
        write list = Administrator, root
        directory mask = 0775
        browsable = yes
        guest ok = no
        force group = ntadmin
        create mask = 0664
        directory mask = 0775
        printable = no
```

We make the following entries in this file as highlighted in Example 2-2.

- `workgroup = ITSOSMB`

  This entry indicates the name of the Windows NT domain.

- `netbios name = LinuxOni5`

  This entry is the NetBIOS name of the Samba server. This is the name you see in network neighborhood on Windows clients.

- `security = domain`

  This entry means that we are making Samba a member of the Windows NT domain.

- `wins server = 192.168.2.3`

  We type this entry because we are using WINS services from the Windows NT PDC.

- `idmap uid = 10000-20000`

  This entry indicates the range of UID that winbind uses to map NT users to Linux users.

- `idmap gid = 10000-20000`

  This entry indicates the range of the GID that winbind uses to map NT groups to Linux groups.

- `winbind separator = +`

  The winbind separator option allows you to specify how NT domain names and user names are combined into Linux user names when presented to users. By default, winbind uses the traditional back slash (\) separator so that Linux user names look like DOMAIN\username.

  In some cases, this \ separator may cause problems because the character has special meaning in Linux shells. In this case, you can use the winbind separator option to specify an alternative separator character. Good alternatives may be to use the forward slash (/), although it conflicts with the UNIX directory separator, or to use the plus sign (+). The + character appears to be the best choice for 100% compatibility with existing Linux utilities. However, it may be an aesthetically bad choice depending on your needs.

2.4 Testing Samba in the domain

Now, let's verify that everything is working as we intended.

1. Log in as the domain `Administrator` as shown in Example 2-3.

Example 2-3 Logging in as the domain Administrator

```
rchas10s:~# net rpc join -U Administrator
Password:
Joined domain ITSOSMB.
rchas10s:~#
```

2. Start Samba as shown in Example 2-4.

Example 2-4 Starting Samba

```
rchas10s:~ # rcnmb start
Starting Samba NMB daemon                    done

rchas10s:~ # rcsmb start
Starting Samba SMB daemon                    done

rchas10s:~ # rcwinbind start
Starting Samba WINBIND daemon                done
```

Confirm whether winbind can resolve the names of domain users. Run the **wbinfo** command as shown in Example 2-5. The **wbinfo -u** command lists all users that are available in the Windows NT domain for which the winbind daemon is operating.

Example 2-5 Running the wbinfo -u command

```
rchas10s:~ # wbinfo -u
ITSOSMB+Administrator
ITSOSMB+farah
ITSOSMB+fin1
ITSOSMB+fin2
ITSOSMB+fin3
ITSOSMB+freddy
ITSOSMB+Guest
ITSOSMB+hrd1
ITSOSMB+IUSR_ITSONT4
ITSOSMB+operator
ITSOSMB+Redbook
ITSOSMB+rehan
ITSOSMB+rumaisa
ITSOSMB+shehzad
ITSOSMB+stacey
ITSOSMB+user1
ITSOSMB+user2
ITSOSMB+user3
ITSOSMB+user4
ITSOSMB+vaclav
ITSOSMB+vaseem
ITSOSMB+yessong
ITSOSMB+zeeshan
```

3. To confirm whether winbind can resolve the names of domain groups, run the **wbinfo** command again. This time, change the parameter to -g as shown in Example 2-6. The **wbinfo -g** command lists all groups available in the Windows NT domain for which the Samba daemon is operating.

Example 2-6 Running the wbinfo -g command

```
rchas10s:~ # wbinfo -g
BUILTIN+System Operators
BUILTIN+Replicators
BUILTIN+Guests
BUILTIN+Power Users
BUILTIN+Print Operators
BUILTIN+Administrators
BUILTIN+Account Operators
BUILTIN+Backup Operators
BUILTIN+Users
ITSOSMB+Domain Admins
ITSOSMB+Domain Guests
ITSOSMB+Domain Users
```

2.4.1 Testing the availability of the Samba shares

You can now login on Windows NT client machines and test the availability of the shares provided by Samba.

1. On the Windows client, double-click the **My Network Places** icon on your desktop.
2. You should see the Itsosmb domain as shown in Figure 2-3. Double-click **Itsosmb**.

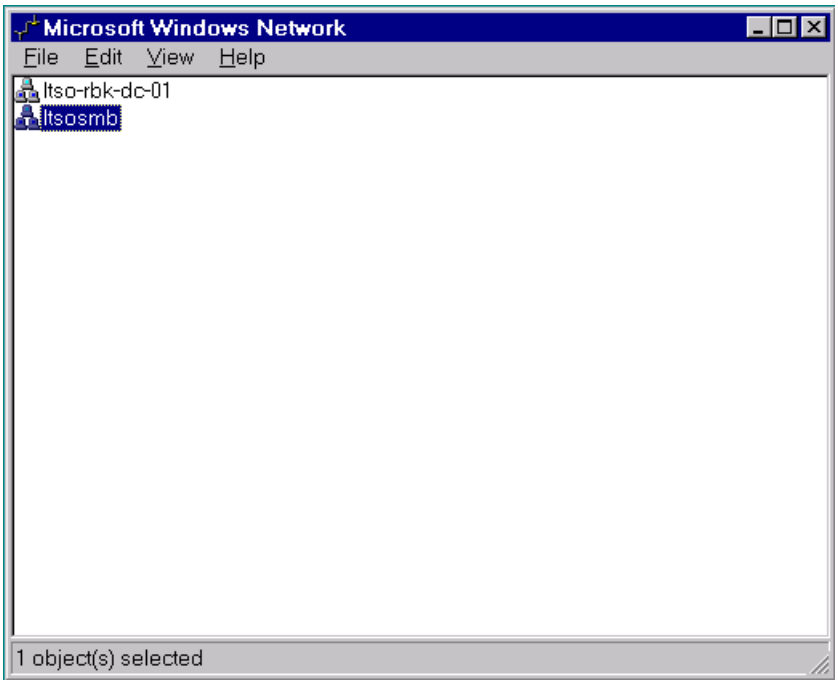


Figure 2-3 Testing the Samba share: My Network Places

3. The object identified as Linuxoni5 (see Figure 2-4) is the Samba server on @server i5. Double-click the **Linuxoni5** icon.

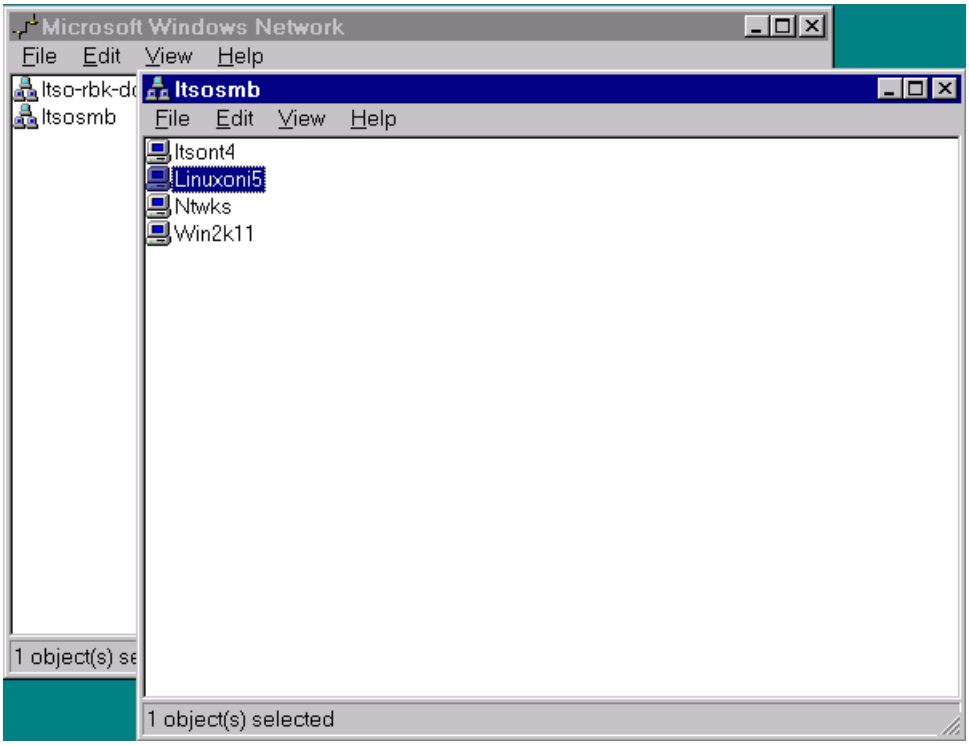


Figure 2-4 Testing the Samba share: Accessing the Itsosmb domain

All shares from this user of ITSOSMB should appear in the window as shown in Figure 2-5. One of the shares is the personal home directory for this user.

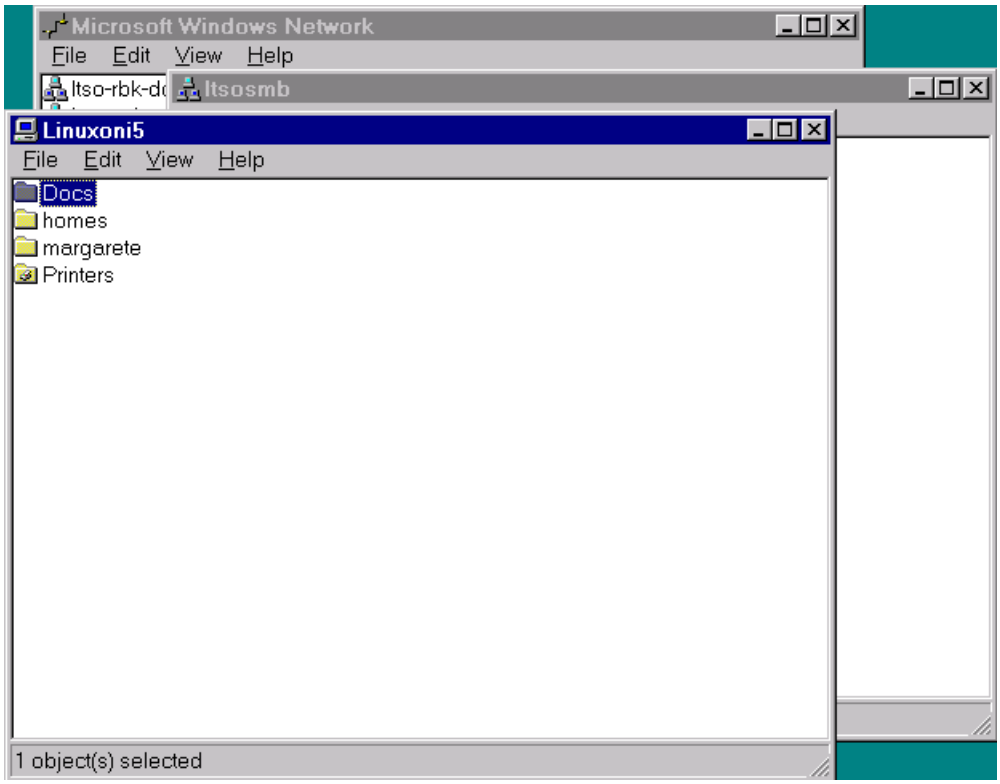


Figure 2-5 Testing the Samba share: All shares are visible

2.4.2 Setting Samba to autostart with at system initialization

Now that everything is running correctly as planned, make Samba automatically start at a system initialization. To make the services run whenever the Linux partition boots or restarts, type the commands as shown in Example 2-7. The **chkconfig** command is used to manipulate the runlevel links at boot time.

Example 2-7 Setting Samba to autostart at system initialization

```
rchas10s:~# chkconfig nmb on
rchas10s:~# chkconfig smb on
rchas10s:~# chkconfig winbind on
```

3

Migrating a Windows AD member to a Linux Samba-3 based AD member on eServer i5

This chapter takes you through the steps to migrate the Active Directory member, of your Microsoft file and print server, to an Active Directory member on @server i5 based on Linux Samba Version 3 (Samba-3). It covers the case of Windows and Samba coexistence. You learn how to integrate Samba in an existing Active Directory domain. This enables you to keep using the domain control services of Active Directory, but replace the Windows file and print servers with Linux Samba-3.

3.1 Scenario description

A Linux server running Samba-3 with a Kerberos client can provide file and print serving integration in an Active Directory structure using Kerberos.

3.1.1 Prerequisites

Prior to implementing this scenario, you must ensure that the following prerequisites are in place:

- The Active Directory is already implemented and working.
- You have secured and patched your Windows system.
- You have installed Linux on @server i5, with the Samba-3 and Kerberos packages.
- You have at least one Windows-based machine to do testing.
- You have root access to the system to which you are configuring Samba.
- You have domain administrative access to the Active Directory.

3.1.2 General settings

The configuration scenario presented in this chapter is based on the following settings:

- All the machines including the Linux partition are in the same subnet 192.168.2.0/24.
- The Windows workstations that are used include Windows NT4 workstation and Windows 2000 Professional.
- The Windows 2000 Active Directory Server is used.
- The Linux distribution that is used is SUSE LINUX Enterprise Server 9 (SLES9) for @server i5.

Note: We used SLES9 and Microsoft Windows 2000 Active Directory, so all examples that are shown reflect those products. The same concept applies if you use RedHat Enterprise Linux (RHEL4), Microsoft Windows 2003 Active Directory, or both. The configuration files should be the same. The only differences would be in Linux distribution particulars, such as how to run the stop and start functions in daemons.

3.1.3 Specific settings for Windows and Linux

For Windows, the scenario used the following settings:

- Name of the Active Directory Domain: `ITSO.COM`
- Name of the Windows 2000 DC: `ITSO-RBK-DC-01` (`192.168.2.1`)
- Name of the Windows 2000 Professional client: `ITSO-RBK-2K` (`192.168.2.2`)
- Name of the Windows NT4 Workstation: `NTWKS` (`192.168.2.4`)

For Linux, in this case, the Linux partition has an IP address that is configured on interface eth1 (192.168.2.5).

3.1.4 Installation checklist

Prior to running this scenario, the following items were installed or verified as operational:

- Domain Name System (DNS) service is an integral part of Active Directory Services (ADS). The ADS domain, named ITSO.COM, must be installed and configured with a properly configured DNS service.
- The Windows clients must be installed and part of the Active Directory environment.

- SLES9 must be installed and operational.
- The Samba-3 and Kerberos packages must be installed.
- All the machines must be able to resolve each other's names using DNS.

3.2 Step-by-step migration guide

This section guides you step-by-step through the integration of a Samba server into an existing Windows ADS environment.

3.2.1 Task 1: Compatibility checklist

The Samba-3 package must be built with Kerberos and LDAP support libraries. The package that shipped with SLES9 is configured with both of these libraries by default. To confirm whether Samba-3 is built with Kerberos support, on a Linux terminal session, type:

```
/usr/sbin/smbd -b | grep KRB
```

You should see a confirmation panel like the one in Figure 3-1.

```
Linuxoni5:~ # /usr/sbin/smbd -b | grep KRB
   HAVE_KRB5_H
   HAVE_ADDR_TYPE_IN_KRB5_ADDRESS
   HAVE_KRB5
   HAVE_KRB5_AUTH_CON_SETKEY
   HAVE_KRB5_FREE_DATA_CONTENTS
   HAVE_KRB5_GET_DEFAULT_IN_TKT_ETYPES
   HAVE_KRB5_GET_PW_SALT
   HAVE_KRB5_KEYBLOCK_KEYVALUE
   HAVE_KRB5_KEYTAB_ENTRY_KEYBLOCK
   HAVE_KRB5_MK_REQ_EXTENDED
   HAVE_KRB5_PRINCIPAL_GET_COMP_STRING
   HAVE_KRB5_SET_DEFAULT_IN_TKT_ETYPES
   HAVE_KRB5_STRING_TO_KEY
   HAVE_KRB5_STRING_TO_KEY_SALT
   HAVE_LIBKRB5
   KRB5_PRINC_REALM_RETURNS_REALM
```

Figure 3-1 Confirmation panel showing that Samba is built with Kerberos support

Similarly to confirm that LDAP support is available, type:

```
/usr/sbin/smbd -b | grep LDAP
```

Then you should see a confirmation panel like the one in Figure 3-2.

```
Linuxoni5:~ # /usr/sbin/smbd -b | grep LDAP
   HAVE_LDAP_H
   HAVE_LDAP
   HAVE_LDAP_DOMAIN2HOSTLIST
   HAVE_LDAP_INIT
   HAVE_LDAP_INITIALIZE
   HAVE_LDAP_SET_REBIND_PROC
   HAVE_LIBLDAP
   LDAP_SET_REBIND_PROC_ARGS
```

Figure 3-2 Confirmation panel showing that Samba is built with LDAP support

Having confirmed that Kerberos and LDAP support are built into Samba, we now need to configure three main components:

- Kerberos configuration file /etc/krb5.conf
- Name service switch (NSS) configuration file /etc/nsswitch.conf
- Samba configuration file /etc/samba/smb.conf

3.2.2 Task 2: Configuring Kerberos

The Kerberos configuration file is /etc/krb5.conf. For our scenario, the Active Directory domain ITSO.COM has the realm ITSO.COM. The Windows 2000 Server is the Kerberos Distribution Center (KDC) at the IP address 192.168.2.1. The configuration file should have the contents as shown in Example 3-1.

Example 3-1 /etc/krb5.conf for Kerberos configuration

```
[libdefaults]
   ticket_lifetime = 24000
   default_realm = ITSO.COM
   forwardable = true
   clockskew = 300

[realms]
   ITSO.COM = {
      kdc = 192.168.2.1
      admin_server = 192.168.2.1
      kpasswd_server = 192.168.2.1
      default_domain = itso.com
   }

[domain_realm]
   .itso.com = ITSO.COM
   itso.com = ITSO.COM

[logging]
   default = SYSLOG:NOTICE:DAEMON
   kdc = FILE:/var/log/kdc.log
   kadmind = FILE:/var/log/kadmind.log

[appdefaults]
   pam = {
#     ticket_lifetime = 1d
      renew_lifetime = 1d
      forwardable = true
      proxiable = false
      retain_after_close = false
      minimum_uid = 0
      debug = false
   }
```

We make the following entries as highlighted in Example 3-1:

- `realm`

  This entry indicates a section that describes where to find the kerberos servers.

- `domain_realm`

  This section provides a translation from a host name to the Kerberos realm name for the services provided by that host. It is used to give a fully qualified domain name.

Attention: Kerberos is case sensitive, so you must use care when working in the /etc/krb5.conf file. ADS realms for Kerberos are always in uppercase, as in ITSO.COM in Example 3-1.

After you configure Kerberos, the communication between Linux Server and Active Directory Server is available.

3.2.3 Task 3: Configuring the name service switch

The NSS configuration file is /etc/nsswitch.conf. Configuration in this file, as shown in Example 3-2, provides control for the user and group name resolutions to be done by different sources.

Example 3-2 /etc/nsswitch.conf for NSS control

```
#
# /etc/nsswitch.conf
#
# An example Name Service Switch config file.


passwd: files winbind
group:  files winbind

hosts:  files dns wins
networks:       files dns

services:       files
protocols:      files
rpc:   files
ethers:files
netmasks:       files
netgroup:       files
publickey:files

bootparams:     files
automount:      files
aliases:        files
```

As shown in the file in Example 3-2, we add the entry `windind`. This entry is used to resolve user and group information from Microsoft Windows 200X ADS.

3.2.4 Task 4: Configuring Samba

The Samba configuration file is /etc/samba/smb.conf. The parameters in this file determine the behavior of the Samba service. This file should have the contents as shown in Example 3-3.

Example 3-3 /etc/samba/smb.conf for Samba configuration

```
[global]
   workgroup = ITSO
   realm = ITSO.COM
   security = ADS
   netbios name = Linuxoni5
   password server = 192.168.2.1
   os level = 10
```

```
   socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
   printing = cups
   printcap name = cups
   username map = /etc/samba/smbusers
   server string = Samba on POWER Linux with ADS
   interfaces = eth1, lo
   encrypt passwords = yes
   bind interfaces only = yes
   log file = /var/log/samba/%m
   max log size = 1024
   log level = 2
   idmap uid = 10000-20000
   idmap gid = 10000-20000
   ldap ssl = no
   template primary group = "Domain Users"
   template shell = /bin/bash
   winbind separator = +
   winbind use default domain = yes
   unix charset = LOCALE

[Docs]
   comment = Docs for every body to Browse
   path = /usr/share/doc
   public = yes
   readonly = yes
   guest ok = yes

[printers]
   comment = Samba Printer Spool
   path = /var/spool/samba
   printable = yes
   browseable = no
   guest ok = yes

[print$]
   comment = Printer Drivers
   path = /var/lib/samba/drivers
   write list = Administrator, root
   create mask = 0664
   directory mask = 0775
   browseable = yes
   guest ok = no
   printable = no
```

We make the following entries as highlighted in Example 3-3.

- `workgroup = ITSO`

  A simple grouping of computers used in Windows is intended to help users find such things as printers and shared folders within that group. Workgroups in Windows do not offer the centralized user accounts and authentication that are offered by domains.

- `realm = ITSO.COM`

  This is the Kerberos realm. It is the same as your Active Directory domain of which the host is a member and is always in uppercase.

- `security = ADS`

  This entry identifies the security mode, which must be set to ADS.

- `password server = 192.168.2.1`

  This entry indicates the IP address of the Active Directory domain controller which is used on the Kerberos server.

Tip: In addition to the smb.conf file, the root user must exist in the password backend. If you are working with **smbpasswd**, you can add a root user to this database by using the following command:

```
smbpasswd -a root
```

When prompted for the new SMB password, give the password of the root user.

3.2.5 Task 5: Testing the Kerberos and Samba configuration

Having configured all the required services, verify whether they are working as planned.

1. Run the command as shown in Example 3-4 to ensure that Kerberos is functioning properly. When prompted for the password, type the AD domain administrator's password. The output as shown in Example 3-4 confirms that the Kerberos is working.

   Note: In this example with SLES9, the **kinit** command is in the heimdal-tools-0.6.1rc3-55.3 package.

Example 3-4 Checking Kerberos

```
linuxoni5:/etc/samba # /usr/bin/kinit Administrator@ITSO.COM
Administrator@ITSO.COM's Password:
kinit: NOTICE: ticket renewable lifetime is 1 week
```

2. Check for any syntax errors with the smb.conf file using the command as shown in Example 3-5.

Example 3-5 Testparm command

```
inuxoni5:~# testparm
Load smb config files from /etc/samba/smb.conf
Processing section "[netlogon]"
Processing section "[homes]"
Processing section "[docs]"
Processing section "[profiles]"
Processing section "[printers]"
Processing section "[print$]"
Loaded services file OK.
```

   Attention: The output displays any syntax errors that are found. Correct them and run the command again.

3. Although we are working with a fresh installation, to be sure that there are no surprises ahead, we delete any existing cache files as shown in Example 3-6.

Example 3-6 Removing files

```
Linuxoni5:~# rm -f /var/lib/samba/*tdb
Linuxoni5:~# rm -f /etc/samba/secrets.tdb
```

3.2.6 Task 6: Joining Samba to the AD domain

Now we join Samba to the AD domain.

1. Run the command as shown in Example 3-7, which also shows the expected output. When prompted for the password, enter the AD domain administrator's password.

   The output shows that Samba has successfully joined the AD domain.

Example 3-7 Joining Samba

```
linuxoni5:/etc/samba # net ads join -UAdministrator
Administrator's password:
Using short domain name -- ITSO
Joined 'LINUXONI5' to realm 'ITSO.COM'
```

2. Start Samba and the required winbind services as shown in Example 3-8.

Example 3-8 Starting Samba

```
Linuxoni5:~# rcnmb start
Linuxoni5:~# rcsmb start
Linuxoni5:~# rcwinbind start
```

Note: If your Samba service was started before joining Samba to Active Directory, you need to restart winbind by using the following command:

```
rcwinbind restart
```

3.3 Verifying the scenario implementation

Now you must verify that the implementation is correct. In the following sections, we offer two test scenarios.

3.3.1 Confirming the scenario

Before we can see the Samba shares on the client machines, we must perform the following steps.

1. Confirm whether winbind can resolve the names of users and groups by running the following command:

   ```
   Linuxoni5:~#/etc/samba # wbinfo -u
   ```

   Example 3-9 shows the list of local and Active Directory users.

Example 3-9 Name resolution of users and groups via winbind

```
linuxoni5:/etc/samba # wbinfo -u
vaseem
freddy
stacey
vaclav
yessong
rumaisa
Administrator
Guest
TsInternetUser
IUSR_ITSO2000
IWAM_ITSO2000
krbtgt
```

```
NTWKS$
ITSO-RBK2K$
HOST/linuxi5new
ITSO-REDBOOK-DC$

linuxi5new:/etc/samba # wbinfo -g
Domain Computers
Domain Controllers
Schema Admins
Enterprise Admins
Cert Publishers
Domain Admins
Domain Users
Domain Guests
Group Policy Creator Owners
DnsUpdateProxy
Management
Non-Management
linuxoni5:/etc/samba #
```

2. Confirm the user name resolution via NSS by running the following command:

   ```
   linuxoni5:/etc/samba # getent passwd
   ```

   Example 3-10 shows the list of local and Active Directory groups.

Example 3-10 Confirmation of user name resolution via NSS

```
linuxoni5:/etc/samba # getent passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/bin/bash
daemon:x:2:2:Daemon:/sbin:/bin/bash
lp:x:4:7:Printing daemon:/var/spool/lpd:/bin/bash
mail:x:8:12:Mailer daemon:/var/spool/clientmqueue:/bin/false
news:x:9:13:News system:/etc/news:/bin/bash
uucp:x:10:14:Unix-to-Unix CoPy system:/etc/uucp:/bin/bash
games:x:12:100:Games account:/var/games:/bin/bash
man:x:13:62:Manual pages viewer:/var/cache/man:/bin/bash
at:x:25:25:Batch jobs daemon:/var/spool/atjobs:/bin/bash
wwwrun:x:30:8:WWW daemon apache:/var/lib/wwwrun:/bin/false
ftp:x:40:49:FTP account:/srv/ftp:/bin/bash
postfix:x:51:51:Postfix Daemon:/var/spool/postfix:/bin/false
sshd:x:71:65:SSH daemon:/var/lib/sshd:/bin/false
ntp:x:74:65534:NTP daemon:/var/lib/ntp:/bin/false
ldap:x:76:70:User for OpenLDAP:/var/lib/ldap:/bin/bash
nobody:x:65534:65533:nobody:/var/lib/nobody:/bin/bash
teresa:x:1000:100:Maria Marulanda:/home/teresa:/bin/bash
vaseem:x:10000:10000:Vaseem Ansari:/home/ITSO-RBK-DC-01/vaseem:/bin/bash
freddy:x:10001:10000:Freddy Cruz:/home/ITSO-RBK-DC-01/freddy:/bin/bash
stacey:x:10002:10000:Stacey Johnson:/home/ITSO-RBK-DC-01/stacey:/bin/bash
vaclav:x:10003:10000:Vaclav Mat:/home/ITSO-RBK-DC-01/vaclav:/bin/bash
yessong:x:10004:10000:Yessong Johng:/home/ITSO-RBK-DC-01/yessong:/bin/bash
rumaisa:x:10005:10000:Rumaisa Ansari:/home/ITSO-RBK-DC-01/rumaisa:/bin/bash
Administrator:x:10006:10000:Administrator:/home/ITSO-RBK-DC-01/Administrator:/bin/bash
Guest:x:10007:10000:Guest:/home/ITSO-RBK-DC-01/Guest:/bin/bash
TsInternetUser:x:10008:10000:TsInternetUser:/home/ITSO-RBK-DC-01/TsInternetUser:/bin/bash
IUSR_ITSO2000:x:10009:10000:IUSR_ITSO2000:/home/ITSO-RBK-DC-01/IUSR_ITSO2000:/bin/bash
IWAM_ITSO2000:x:10010:10000:IWAM_ITSO2000:/home/ITSO-RBK-DC-01/IWAM_ITSO2000:/bin/bash
krbtgt:x:10011:10000:krbtgt:/home/ITSO-RBK-DC-01/krbtgt:/bin/bash
NTWKS$:x:10012:10001:NTWKS:/home/ITSO-RBK-DC-01/NTWKS_:/bin/bash
```

```
ITSO-RBK2K$:x:10013:10001:ITSO-RBK2K:/home/ITSO-RBK-DC-01/ITSO-RBK2K_:/bin/bash
HOST/linuxi5new:x:10014:10001:linuxi5new:/home/ITSO-RBK-DC-01/HOST/linuxi5new:/bin/bash
ITSO-REDBOOK-DC$:x:10015:10002:ITSO-REDBOOK-DC:/home/ITSO-RBK-DC-01/ITSO-REDBOOK-DC_:/bin/b
ash
```

3. Confirm the group name resolution via NSS by running the following command:

   ```
   linuxoni5:/etc/samba # getent group
   ```

   Example 3-11 shows the output of the command.

Example 3-11 Confirmation of group names resolution via NSS

```
linuxoni5:/etc/samba # getent group
root:x:0:
bin:x:1:daemon
daemon:x:2:
sys:x:3:
tty:x:5:
disk:x:6:
lp:x:7:
www:x:8:
kmem:x:9:
wheel:x:10:
mail:x:12:
news:x:13:
uucp:x:14:teresa
shadow:x:15:
dialout:x:16:teresa
audio:x:17:teresa
floppy:x:19:
cdrom:x:20:
console:x:21:
utmp:x:22:
at:!:25:
public:x:32:
video:x:33:teresa
games:x:40:
xok:x:41:
trusted:x:42:
modem:x:43:
ftp:x:49:
postfix:!:51:
maildrop:!:59:
man:x:62:
sshd:!:65:
ldap:!:70:
ntadmin:!:71:
nobody:x:65533:
nogroup:x:65534:nobody
users:x:100:
Domain Computers:x:10001:
Domain Controllers:x:10002:
Schema Admins:x:10008:Administrator
Enterprise Admins:x:10006:Administrator
Cert Publishers:x:10010:
Domain Admins:x:10009:Administrator
Domain Users:x:10000:
Domain Guests:x:10011:Guest
Group Policy Creator Owners:x:10007:Administrator
DnsUpdateProxy:x:10012:
```

```
Management:x:10005:yessong,vaseem
Non-Management:x:10013:vaclav,stacey,freddy
linuxoni5:/etc/samba #
```

4. Confirm that the Samba-3 and AD server are communicating via Kerberos by running the following command:

   ```
   linuxoni5:/etc/samba # net ads info
   ```

   As shown in Example 3-12, these tests confirm that Samba is now integrated with the AD server and is talking to the AD server by using Kerberos.

Example 3-12 Confirmation of Samba-3 and AD server communication via Kerberos

```
linuxoni5:/etc/samba # net ads info
LDAP server: 192.168.2.1
LDAP server name: itso-redbook-dc
Realm: ITSO.COM
Bind Path: dc=ITSO,dc=COM
LDAP port: 389
Server time: Mon, 09 Aug 2004 18:15:18 GMT
KDC server: 192.168.2.1
Server time offset: -123
linuxi5new:/etc/samba #
```

3.3.2 Testing the Samba shares

Now we can login on any of the client machines and test the availability of the shares provided by Samba.

1. On a Windows 2000 Professional client, from your desktop, double-click **My Network Places**.
2. Double-click the **Microsoft Windows Network** icon.
3. In the Microsoft Windows Network panel (Figure 3-3), double-click the **Itso** domain.

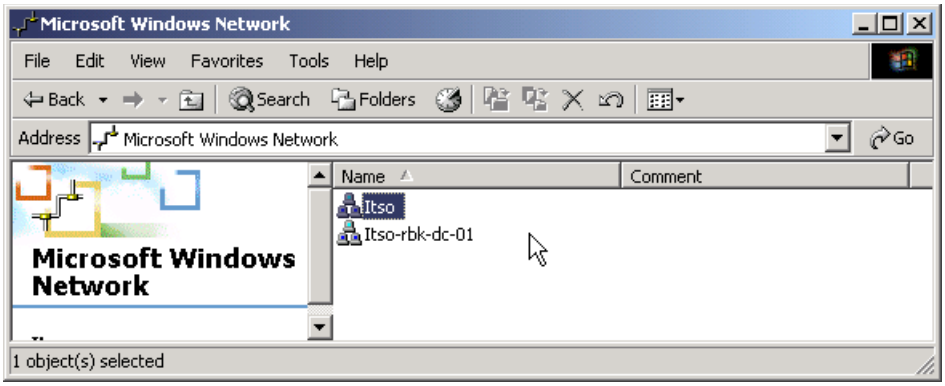


Figure 3-3 Domain ITSO in Microsoft Windows Network

4. In the next window (Figure 3-4), double-click the Samba server **Linuxi5new** in the list.

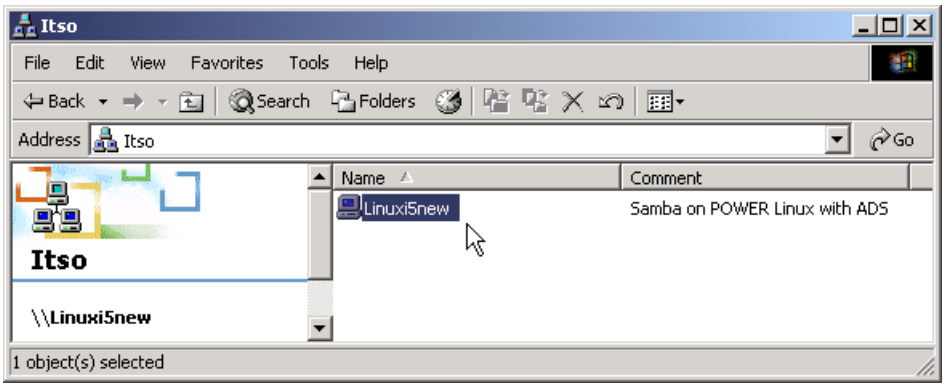


Figure 3-4 Samba server in the ADS domain Itso

5. Next you see the file shares that are made available on the Linuxi5new Samba server (see Figure 3-6). Double-click the **Docs** share.

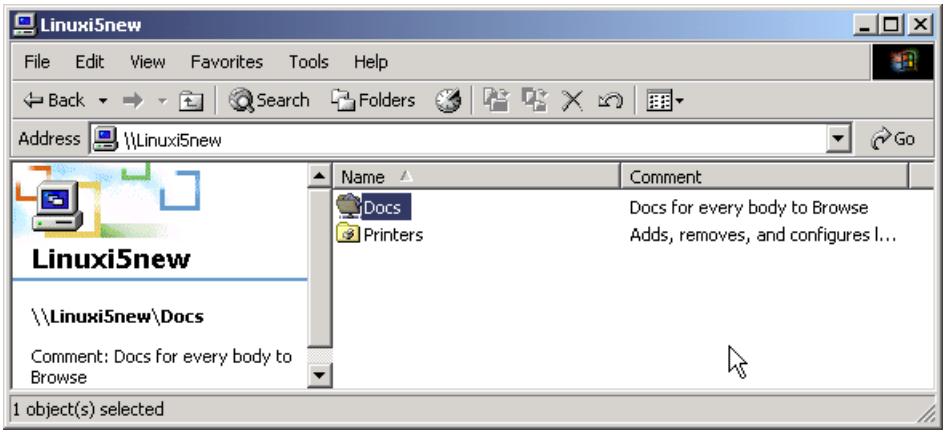


Figure 3-5 Samba shares

Based on the access privileges of the logged in user, you can explore the shares from the next window (see Figure 3-6).

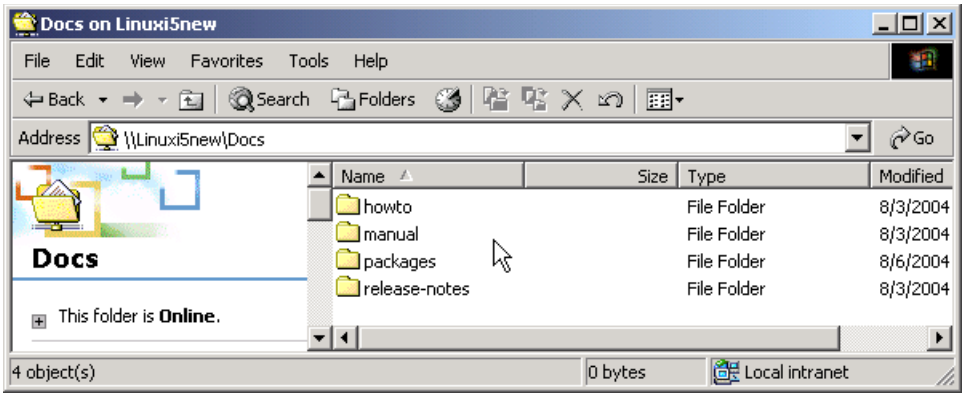


Figure 3-6 Exploring Samba's Docs share

3.3.3 Defining Samba to autostart with system reboot

Now everything is running correctly as planned. Set Samba so that it starts automatically on a system reboot. To make the services auto run whenever the Linux partition boots or restarts, type:

```
#linuxoni5:~# chkconfig nmb on
#linuxoni5:~# chkconfig smb on
#linuxoni5:~# chkconfig winbind on
```

File and Print Serving with Linux on IBM @server i5

Redpaper

Learn the benefits of migrating file and print serving workloads using Linux on @server i5

Replace Microsoft Windows-based services with Linux Samba

Create a coexistence of Active Directory Server and Linux Samba

This IBM Redpaper introduces options for migrating a Microsoft Windows-based file and print serving workload to a Linux-based Samba server on the IBM @server i5. It is written to help administrators who are in charge of providing file and print services to their Windows clients and who are considering such a migration project.

To explain the migration options, this paper presents the following three scenarios from the migration implementation perspective:

- Replacement of Windows NT-based services of file and print serving, as well as domain controller functions, with Linux Samba
- Coexistence of the Windows-based domain controller function with Linux Samba, which provides file and print serving workload
- Coexistence of Windows-based Active Directory Server with Linux Samba

For these scenarios, you see a before and after view of the migration environment. Then you follow the migration process step-by-step, and learn about the configuration files and commands to run.

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