

Making the Migration to Linux using Vampire

Matt Skipton

Technology Specialist
Datacenter & Workgroup
Novell, Inc.



Novell®

Agenda

- Why make the migration
- What is Samba/Vampire
- Migration Overview
 - Steps to Convert
- Live Migration
 - Detailed Steps
- Other Features, Options, and Gotha's
 - Additional Resources
- Q&A

Disclaimer

- There are infinite ways to accomplish this task. There are also infinite environmental “issues” that can crop up. This is one method that has worked for me many times. As usual, Your Mileage May Vary (YMMV).

Why Make the Migration

Why Make the Migration

- NT is no longer supported by Microsoft
 - <http://www.microsoft.com/ntserver/ProductInfo/Availability/Retiring.asp>
- Linux is spreading in the datacenter
 - Running windows authentication on linux takes advantage of existing knowledge and skills
- Much cheaper than a move to AD
 - no per-user licensing costs
- Easy backup and recovery for authentication system
 - much simpler than AD

What is Samba and Vampire

What is Samba

- As the front page at samba.org says, "Samba is an Open Source/Free Software suite that provides seamless file and print services to SMB/CIFS clients." Samba is freely available, unlike other SMB/CIFS implementations, and allows for interoperability between Linux/Unix servers and Windows-based clients.
 - Samba-3 by Example explains further, saying:
 - > Samba is software that can be run on a platform other than Microsoft Windows, for example, UNIX, Linux, IBM System 390, OpenVMS, and other operating systems. Samba uses the TCP/IP protocol that is installed on the host server. When correctly configured, it allows that host to interact with a Microsoft Windows client or server as if it is a Windows file and print server.
 - From The Official Samba HOWTO:
 - > The goal behind the project is one of removing barriers to interoperability.

Novell's Involvement with Samba

- Samba is one of the many open source projects that Novell is a significant contributor to.
 - In may of 2005 Novell hired Jeremy Allison, one of the primary developers of Samba
 - > In an interview with eWeek Jeremy said
 - » "Novell's known for file sharing, which is what I do on a day-to-day basis," Allison said in an interview with eWEEK. "There is just a very good fit with what I do and what Novell wanted."
 - ~ <http://www.eweek.com/article2/0,1759,1790391,00.asp>
 - > Jeremy will continue to work on the Samba project and he will be able to release all of his work as Open Source
 - Novell also employs other primary samba developers like Guenter Deschner and Lars Müller
 - Novell is committed to Open Source and projects like Samba

What is Vampire

- One command line option included in the Samba suite
 - Part of net rpc commands
- Allows you to suck the users, groups, and machine accounts from a windows NT environment
 - Hmm, I wonder where the term vampire came from??
- Allows a transition to samba without touching windows workstations

Samba Config File Overview

There are multiple sections to any Samba config file. Each is marked by the section name in []

- Global settings go in [global]
 - these can be overridden by settings for a fileshare

```
[global]
workgroup = TUX-NET
printing = cups
printcap name = cups
printcap cache time = 750
cups options = raw
map to guest = Bad User
include = /etc/samba/dhcp.conf
logon path = \\%L\profiles\.msprofile
logon home = \\%L%\%U\.9xprofile
logon drive = P:
```

Samba Config File Overview

- everything else defines a fileshare

[homes]

comment = Home Directories

valid users = %S

browseable = No

read only = No

inherit acls = Yes

[profiles]

comment = Network Profiles Service

path = %H

read only = No

store dos attributes = Yes

create mask = 0600

directory mask = 0700

Samba Files Overview

- smbclient
 - Used to connect to other samba/windows computers
- net
 - There are many options for this command and they allow to to get/set settings and interact with the samba server.
- testparm
 - Used to test your smb.conf for errors.
- rcnmb & rcsmb
 - The SUSE samba startup scripts.
 - rcnmb starts the netbios protocol
 - rcsmb starts the main samba services
- smbpasswd
 - set passwords in the samba system
- pdbedit
 - tool for viewing and editing the samba database

Migration Overview

High Level, What We Need to Do

- Setup samba as a BDC
- Setup OpenLDAP as a storage backend for Samba
- Join the samba BDC to the existing NT domain
- Suck the users, groups, and machine accounts into samba
- Shutdown NT4 server
- Reconfigure Samba to be a PDC
- Reboot windows boxes and test

Assumptions about our environment

- In order to make this session fit in a 1 hour time frame some assumptions had to be made:
- We have a small network with
 - 1 NT PDC
 - 1 NT Fileserver
- We do not want to modify each workstation
- We will use OpenLDAP for our Samba data
 - We do not have time to cover OpenLDAP in depth. There are many books and websites available.

Live Migration

Setup Samba as a BDC – Samba Settings

- Samba configs are stored in `/etc/samba`
- Edit the default `smb.conf` and make sure the following are set
 - `domain master = no`
 - `local master = yes`
 - `domain logons = yes`
- For this session we will be using the `ldap` backend
 - `passdb backend = ldapsam://127.0.0.1`
- Setup your log files
 - SLES defaults to `/var/log/samba/log.smb` and `log.nmb`
 - Log level 2 gives us about the right amount of logging for getting setup. After that you may want to set it to 1
- Make sure the following line has your current NT Domain name in it
 - `workgroup = ntomainname`

Setup Samba as a BDC – LDAP Script Settings



- When using openldap as a samba database you need to use the smbldap scripts provided in the samba docs
 - add user script = `/usr/local/sbin/smbldap-useradd -m %u`
 - delete user script = `/usr/local/sbin/smbldap-userdel %u`
 - add group script = `/usr/local/sbin/smbldap-groupadd -p %g`
 - delete group script = `/usr/local/sbin/smbldap-groupdel %g`
 - add user to group script = `/usr/local/sbin/smbldap-groupmod -m '%u' '%g'`
 - delete user from group script = `/usr/local/sbin/smbldap-groupmod -x '%u' '%g'`
 - set primary group script = `/usr/local/sbin/smbldap-usermod -g '%g' '%u'`
 - add machine script = `/usr/local/sbin/smbldap-useradd -w '%u'`
 - add share command = `/usr/local/sbin/modify_samba_config`
 - delete share command = `/usr/local/sbin/modify_samba_config`
- These scripts can be found in `/usr/share/doc/packages/samba/examples/LDAP/smbldap-tools-0.9.1` after you install the samba-doc package from yast

Setup Samba as a BDC – OpenLDAP Settings



- When using openldap as a samba database you need to set the following options
 - ldap suffix = dc=demonet,dc=com
 - ldap machine suffix = ou=Computers
 - ldap user suffix = ou=Users
 - ldap group suffix = ou=Groups
 - ldap idmap suffix = ou=Users
 - ldap admin dn = cn=Manager,dc=demonet,dc=com

Demo – Setup smb.conf and smbldap scripts

Setup OpenLDAP

- The OpenLDAP config file is `/etc/slapd.conf`
 - The following settings need to be changed or added to the default SLES config.
 - > `include /etc/openldap/schema/nis.schema`
 - > `include /etc/openldap/schema/samba3.schema`
 - > `suffix "dc=demonet,dc=com"`
 - > `rootdn "cn=Manager,dc=demonet,dc=com"`
 - > `rootpw n0vell`

Setup smbldap script settings

- The settings for the smbldap scripts are stored in `/etc/smbldap-tools`
 - `smbldap.conf` needs the following added or changed
 - > `SID="S-1-5-21-2139989288-483860436-2398042574"`
 - » This must be set to your current domains SID
 - > `suffix="dc=demonet,dc=com"`
 - > `sambaUnixIdPooldn="sambaDomainName=demonet,${suffix}"`
 - `smbldap_bind.conf` needs the following added or changed
 - > `slaveDN="cn=Manager,dc=demonet,dc=com"`
 - > `slavePw="n0vell"`
 - > `masterDN="cn=Manager,dc=demonet,dc=com"`
 - > `masterPw="n0vell"`

Setup local ldap authentication

- You need to setup local ldap authentication so samba will work correctly
 - Use yast's ldap client to make the following changes
 - > use ldap
 - > base dn dc=demonet,dc=com
 - > uncheck tls/ssl
 - > advanced button
 - > change base dn to dc=demonet,dc=com
 - > change admin dn to cn=Manager,dc=demonet,dc=com
 - > click "configure user management settings" to test the passwd

Demo – Setup OpenLDAP and smbldap script preferences

Join the Samba BDC to the Existing NT domain

- Run testparm and make sure there are no error and it reports “ROLE DOMAIN BDC”
- Actually join the domain
 - net rpc join -S ntpdc -Uadministrator
- Use server manager on the NT server to make sure that the samba BDC shows up
- Run “net groupmap list” and verify that:
 - Make sure the SID matches the one from the “net rpc getsid” we ran earlier
 - Make sure there are no groups mapped to “-1”

Suck the Users, Groups, and Machine Accounts Into Samba



- Run the “vampire” command
 - `net rpc vampire -S ntpdc -W ntdomain 2>&1 |tee /root/vampire.log`
- Verify the users came over with `pdbedit`
 - `pdbedit -L`
 - or `pdbedit -Lv username` for more details on a user
- Verify the groups came over with `net group`
 - `net groupmap list`
- Check the `vampire.log` for any errors
- Clean up any users who have had profiles or homedirs added that shouldn't have them
 - `pdbedit -r --homedir"" --profile"" administrator`

Clean Up and Verify Unix to nt Group Mappings



- net groupmap list
 - > Domain Admins (S-1-5-21-1385457007-882775198-1210191635-512) -> Domain Admins
 - > Domain Users (S-1-5-21-1385457007-882775198-1210191635-513) -> Domain Users
 - > Domain Guests (S-1-5-21-1385457007-882775198-1210191635-514) -> Domain Guests
 - > Domain Computers (S-1-5-21-1385457007-882775198-1210191635-515) -> Domain Computers
 - > Administrators (S-1-5-32-544) -> Administrators
 - > Print Operators (S-1-5-32-550) -> Print Operators
 - > Backup Operators (S-1-5-32-551) -> Backup Operators
 - > Replicators (S-1-5-32-552) -> Replicators
- Make sure all of our groups made it.

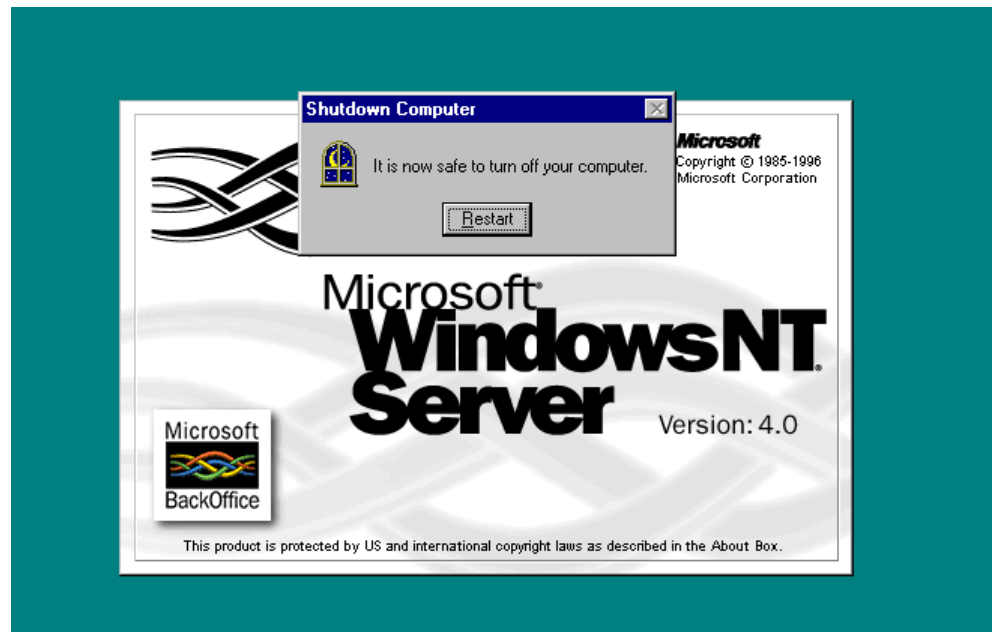
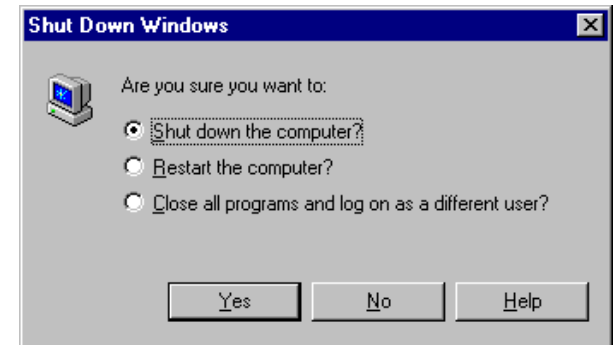
Migrate files and shares to samba

- To migrate a single share
 - There are many ways to accomplish this
 - Some questions worth asking
 - > Are you comfortable with your current security settings
 - > Is your data in need of some restructuring
 - > How important are attributes that are currently on the files
 - The most complete way to migrate files
 - > `net rpc share migrate shares SHARENAME -S SERVERNAME -U Administrator`
 - » You can run into many issues where this will fail
 - The easiest ways to move the files
 - > `smbclient`
 - > `rsync`

Demo – Join the domain and vampire the users

Shutdown NT4 server

- Enough said :)



Reconfigure Samba to be a PDC

- Change 2 lines in /etc/smb.conf
 - domain master = yes
 - wins support = yes
 - > If using wins
 - > you may also need to update your wins server address(s) in your dhcp server
- Check the config again with testparm
 - Make sure the output says ROLE_DOMAIN_PDC
- Restart samba
 - rcsmb restart
 - rcnmb restart
- Make sure samba is scheduled to startup if the linux server reboots
 - chkconfig smb on
 - chkconfig nmb on

Reboot windows boxes and test

- Reboot a windows client and test login, everything should work as before :)
- Including editing user accounts through user manager for domains

Demo – Reconfigure Samba as a PDC and test

Other Features, Options, and Gotha's

Gotcha's

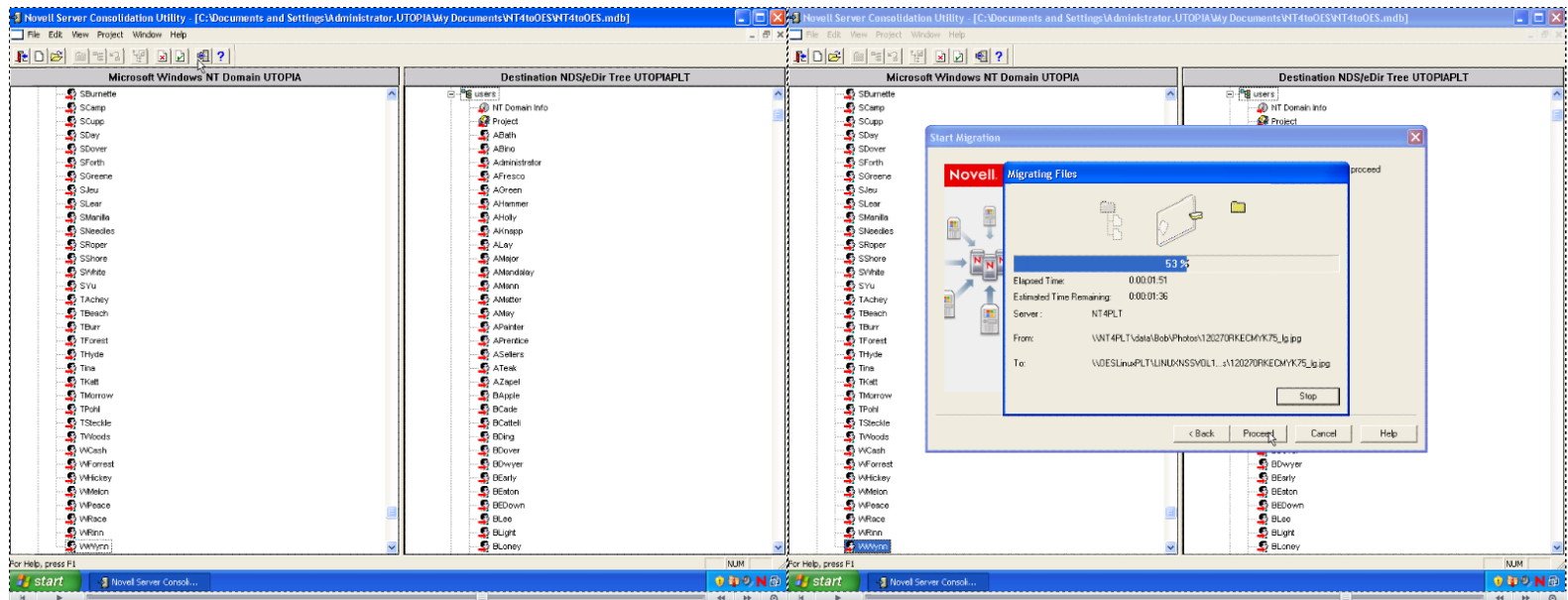
- posix acl issues with file shares
 - backup/restore issues
 - is it turned on for your fs in fstab??
- In all but the smallest environments tdbsam will not scale effectively
 - Novell recommends some form of ldap back-end such as OpenLDAP or eDirectory
 - > The setup of these products can vary from organization to organization and we did not have enough time to cover them in depth in this demonstration. The migration steps would be the same regardless of the backend.

Taking it to the Next Level

- What is Possible
 - Idapsmb scripts for using an LDAP backend
 - ldap backend features and scalability examples
 - Novell® Consulting Example
 - > Migrate a large company with many NT domains to OES-Linux
 - » One domain at a time through a script
 - > The objective of this engagement was to demonstrate OES's ability to provide state-of-the-art file, print, and directory services on a Linux platform (SuSE Linux Enterprise Server 9, while also offering Windows NT4 backward compatibility. In the end, Novell produced a document with setp by step instructions for the customers personell to migrate 1 NT Domain at a time over to OES Linux. The main result was a mile called migrate.pl that asks some questions about the domain and then runs all migration steps.
 - File migration options
 - OES Server Consolidation Tool

Taking it to the Next Level

- OES Server Consolidation Tool
 - Provides an easy to use drag and drop interface to migrate from Windows to OES on Linux. Keeps all file permissions, attributes, and user info intact.



More Info and References

- The Official Samba-3 HOWTO and Reference Guide
 - <http://samba.org/samba/docs/man/Samba-HOWTO-Collection/>
- Samba-3 by Example
 - <http://us5.samba.org/samba/docs/man/Samba-Guide/>
- The official samba website
 - <http://www.samba.org>
- The Linux Samba-OpenLDAP Howto
 - <http://samba.idealx.org/smbldap-howto.en.html>
- My sambafiles.tgz file for this demo
 - <http://demo.stl.novell.com/sambafiles.tgz>

More Info and References

- The openSUSE Samba Howto
 - http://en.opensuse.org/Howto_setup_SUSE_as_SAMBA_PDC_with_OpenLDAP,_DYNDNS_and_CLAM
- Docs installed with Samba
 - /usr/share/doc/packages/samba
- Additional sessions you may be interested in.
 - TUT161 - Using Novell eDirectory For Much More Than Just an LDAP Store - Rick Killpack
 - TUT260 - Performance Tuning and Design of Novell eDirectory to ensure timely identity management for your LDAP applications - Steve Lindsey
 - TUT318 - Using Samba in a Novell Open Enterprise Server Environment - Sander van Vugt

-

Q&A

Novell®

Unpublished Work of Novell, Inc. All Rights Reserved.

This work is an unpublished work and contains confidential, proprietary, and trade secret information of Novell, Inc. Access to this work is restricted to Novell employees who have a need to know to perform tasks within the scope of their assignments. No part of this work may be practiced, performed, copied, distributed, revised, modified, translated, abridged, condensed, expanded, collected, or adapted without the prior written consent of Novell, Inc. Any use or exploitation of this work without authorization could subject the perpetrator to criminal and civil liability.

General Disclaimer

This document is not to be construed as a promise by any participating company to develop, deliver, or market a product. Novell, Inc., makes no representations or warranties with respect to the contents of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All Novell marks referenced in this presentation are trademarks or registered trademarks of Novell, Inc. in the United States and other countries. All third-party trademarks are the property of their respective owners.

