



Samba: Admin & Privileges

John H Terpsta,
CTO

Primastasys Inc

jht@primastasys.com

jht@samba.org



Overview



- About the Author
- Samba Documentation
- Samba: Remote and Local Administration
- Samba: User Rights & Privileges
- The next steps ...



The Author

- Long term Samba Team member
 - General Secretary
- Have written HOWTOs since 1996
- Update to Samba-HOWTO-Collection – 2003
 - In time for Samba-3.0.0
- Samba-3 By Example – 2004
- Second Editions – 2005
 - Released at LinuxWorld Expo – San Francisco '05

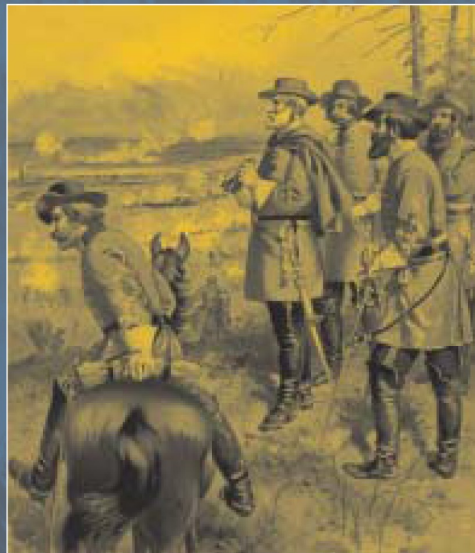


BRUCE PERENS' OPEN SOURCE SERIES

THE OFFICIAL SAMBA-3 HOWTO and Reference Guide

Samba
3.0.20
Series

Second Edition



- Expert information, straight from the source—written by members of the Samba team
- Extensive and detailed explanation of the internal and external capabilities new since the Samba-3.0.11 and later release
- The definitive reference for Samba-3 advanced features and how to use them
- Just what you need to get the most out of your Samba-3 installation

JOHN H. TERPSTRA AND
JELMER R.VERNOOIJ, EDITORS

Foreword by Carl Cargill, Executive Director of Corporate Standards,
Sun Microsystems



BRUCE PERENS' OPEN SOURCE SERIES

SAMBA-3 BY EXAMPLE

Practical Exercises to Successful Deployment

**Samba
3.0.20 and
Later**



Second Edition

- This book is your road map to complete networks, including detailed, step-by-step installation guidelines
- A new chapter to guide your upgrades and updates to the latest versions
- Nothing makes Samba-3 deployment easier than this book, written by the author of the official Samba documentation

JOHN H. TERPSTRA

Foreword by John M. Weathersby, Executive Director,
Open Source Software Institute



User Account Maintenance

- Use the *pdbedit* command to maintain
 - Add, delete, modify user accounts
 - Migrate accounts to/from other backend databases
 - Manage account policies
 - Manage domain access policies



pdbedit – Account Attributes

- Unix username
- NT username
- Account Flags
- User SID
- Primary Group SID
- Full Name
- Home Directory
- Logon Script
- Profile path
- Domain
- Account Description
- Workstations
- Munged Dial String
- Logon/off times
- Password Expiry
- Bad password limits



Usage: *pdbedit* (partial output)

Usage: [OPTION...]

-L, --list	list all users
-v, --verbose	be verbose
-w, --smbpasswd-style	give output in smbpasswd style
-u, --user=USER	use username
-N, --account-desc=STRING	set account description
-f, --fullname=STRING	set full name
-h, --homedir=STRING	set home directory
-D, --drive=STRING	set home drive
-S, --script=STRING	set logon script
-p, --profile=STRING	set profile path
-U, --user-SID=STRING	set user SID or RID
-G, --group-SID=STRING	set group SID or RID
-a, --create	create user
-r, --modify	modify user
-m, --machine	account is a machine account
-x, --delete	delete user
-b, --backend=STRING	use different passdb backend as default



Examples



```
pdbedit --pwd-must-change-time="2010-01-01" --time-format="%Y-%m-%d" vlaan
```

```
pdbedit -P "maximum password age" -C 90  
account policy value for maximum password age was 4294967295
```

```
pdbedit -i smbpasswd -e ldapsam
```



Primary Use: *pdbedit*

- Management of local user accounts
- Management of domain policies
- Not Used for
 - Group Account Managment



The *net* Command

- Can be used across platforms
 - rap, rpc, ads
- Manage Groups
 - two types – local and global (domain)
 - add, delete, modify, list
- Map Linux group to Windows group
 - == creating a Windows group



Handling Group Info

- List groups on remote machine
 - `net rpc group list -S BILBO -U admin%password`
- Add a group to a remote machine
 - `net rpc group add "Marketing" -S FRODO -U admin%password`
- Add a group member
 - `net rpc group addmem "BIGDOM\Engineers" giovanni -S MERLIN -U admin%password`



Mapping UNIX Groups

- Basic
 - `net groupmap modify ntgroup="Domain Admins"`
`unixgroup=root`
 - `net groupmap modify ntgroup="Domain Users"`
`unixgroup=users`
 - `net groupmap modify ntgroup="Domain Guests"`
`unixgroup=nogroup`
 - `net groupmap add ntgroup="Engineers"`
`unixgroup=eng`



Local Group Handling

- Create a local group
 - Can contain user and global group members
 - `net rpc group add Showdogs -L -S MORDON -U admin%password`
- Add domain group to local machine group
 - `net rpc group addmem "Showdogs" "MYDOM\Badboys -S TERMINATOR -U admin %password"`