Remote Management, Windows Tools, & Samba 3.0

Gerald (Jerry) Carter
SAMBA Team
Centeris

jerry@samba.org
http://www.samba.org/
http://www.centeris.com/

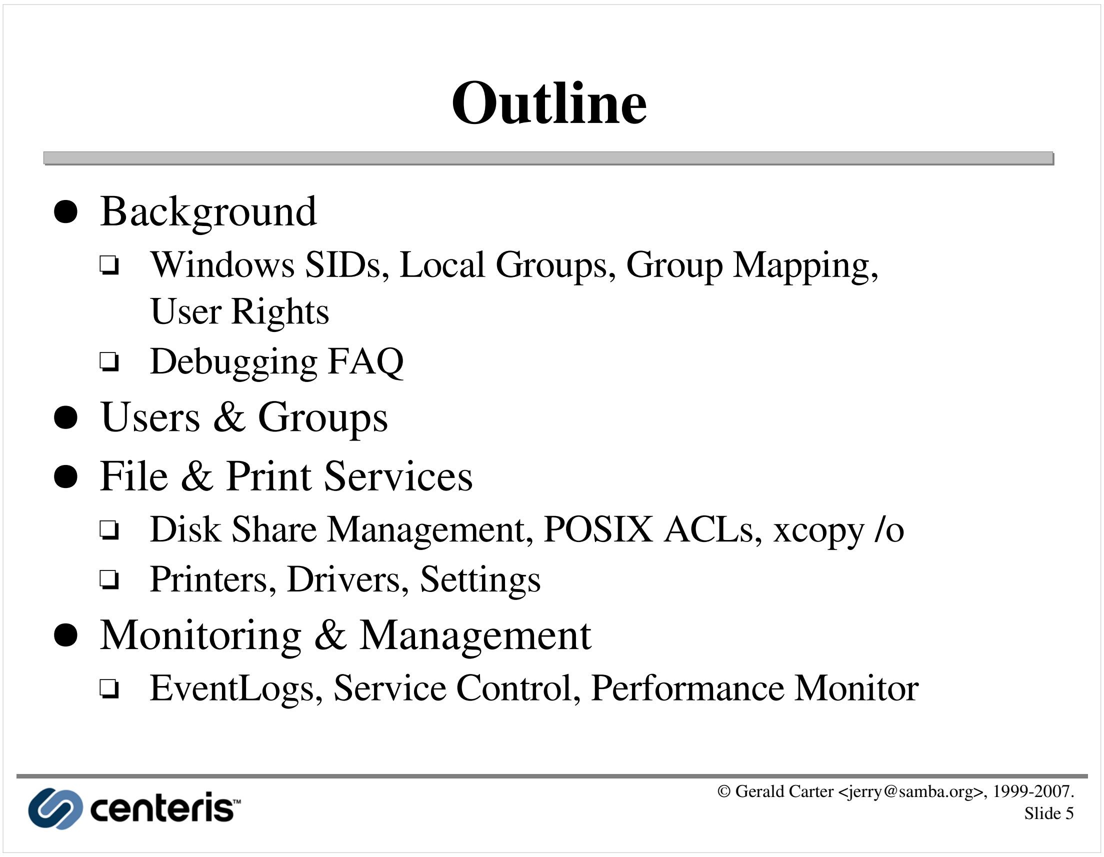
Generalities

- Focus
  - ❑ Making Windows Remote Management tools work with Samba 3.0
  - ❑ Debugging tools that don't work
  - ❑ Examples are based on 3.0.25rc2
- Assumptions
  - ❑ You are comfortable with basic Samba file and print installation and configuration tasks
  - ❑ You are familiar with the basics of Samba member servers and domain controllers

Samba.org Family

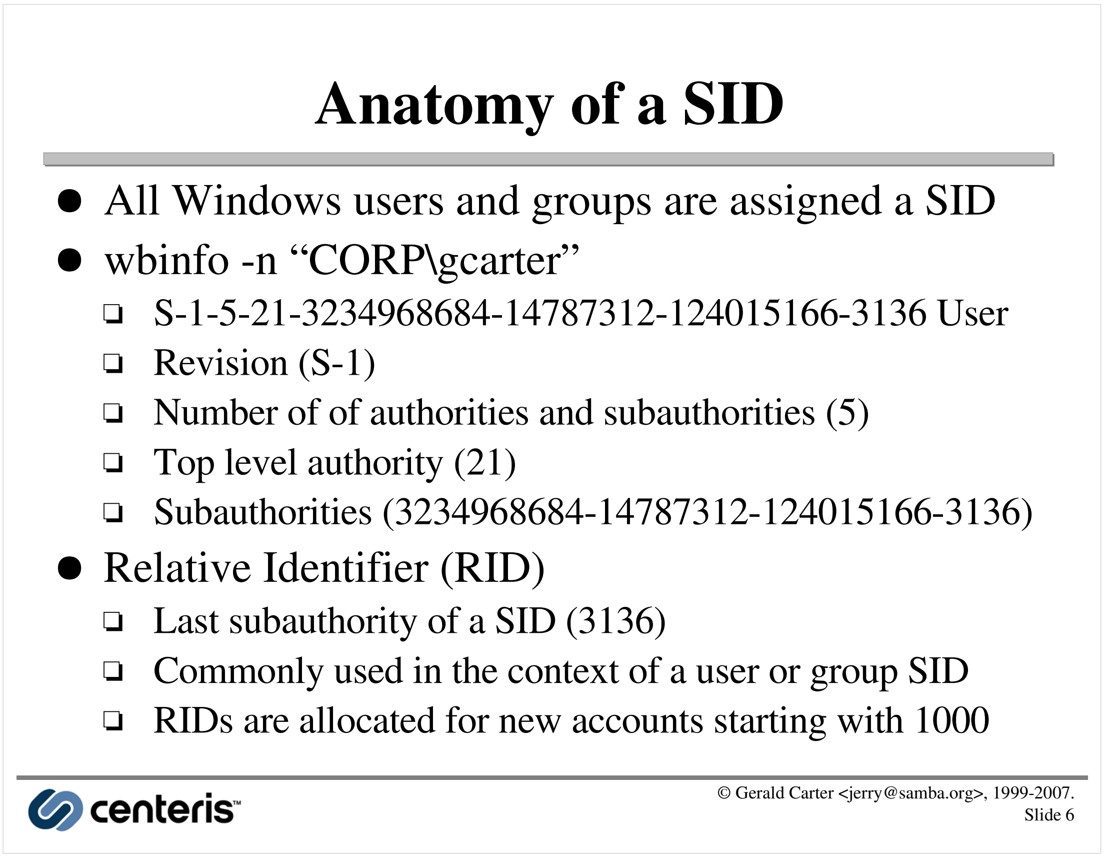
- Main Sites
  - ❑ http://www.samba.org/
  - ❑ http://news.samba.org/
  - ❑ http://wiki.samba.org/
  - ❑ https://bugzilla.samba.org/
- http://www.samba.org/samba/docs/
  - ❑ SHARG, SbE, & “Using Samba” (samba-xxx/docs/)
- http://www.samba.org/samba/security/
  - ❑ Security announcement and related patches
- http://www.samba.org/samba/patches/
  - ❑ Recommended patches

This page intentionally left blank



Outline

- Background
  - ❑ Windows SIDs, Local Groups, Group Mapping, User Rights
  - ❑ Debugging FAQ
- Users & Groups
- File & Print Services
  - ❑ Disk Share Management, POSIX ACLs, xcopy /o
  - ❑ Printers, Drivers, Settings
- Monitoring & Management
  - ❑ EventLogs, Service Control, Performance Monitor



Anatomy of a SID

- All Windows users and groups are assigned a SID
- wbinfo -n “CORP\gcarter”
  - ❑ S-1-5-21-3234968684-14787312-124015166-3136 User
  - ❑ Revision (S-1)
  - ❑ Number of of authorities and subauthorities (5)
  - ❑ Top level authority (21)
  - ❑ Subauthorities (3234968684-14787312-124015166-3136)
- Relative Identifier (RID)
  - ❑ Last subauthority of a SID (3136)
  - ❑ Commonly used in the context of a user or group SID
  - ❑ RIDs are allocated for new accounts starting with 1000

Types of SIDs

- A SID defines a domain of accounts
- Machine (or Windows domain)
  - ❑ S-1-5-21-3234968684-14787312-124015166
- BUILTIN
  - ❑ S-1-5-32-544
- Samba specific SIDs
  - ❑ Unix User (S-1-22-1)
  - ❑ Unix Group (S-1-22-2)

Types of Groups

- Domain Groups
  - ❑ Domain Admins (512), Domain Users (513), Domain Guests (514)
- Local Groups (NT4)
  - ❑ Samba implements the NT4 model of local groups
    - ✔ Native mode AD introduces domain local groups
  - ❑ Local to a specific machine
  - ❑ Can contain users and domain groups
- Well Known Groups
  - ❑ Example: Everyone (S-1-1-0), Authenticated Users (S-1-5-11)

Authorization in Samba

- A user session possesses an
  - ❑ NT token containing a list of SIDs
  - ❑ Unix token containing a list of gids
- Internal authorization checks are performed against a security descriptor using the NT token
  - ❑ Examples: File share acls, service control, printers
- Access to external resources are performed by assuming the identity of the user and asking the underlying OS to perform the access check
  - ❑ Examples: File system access

Log file: NT token

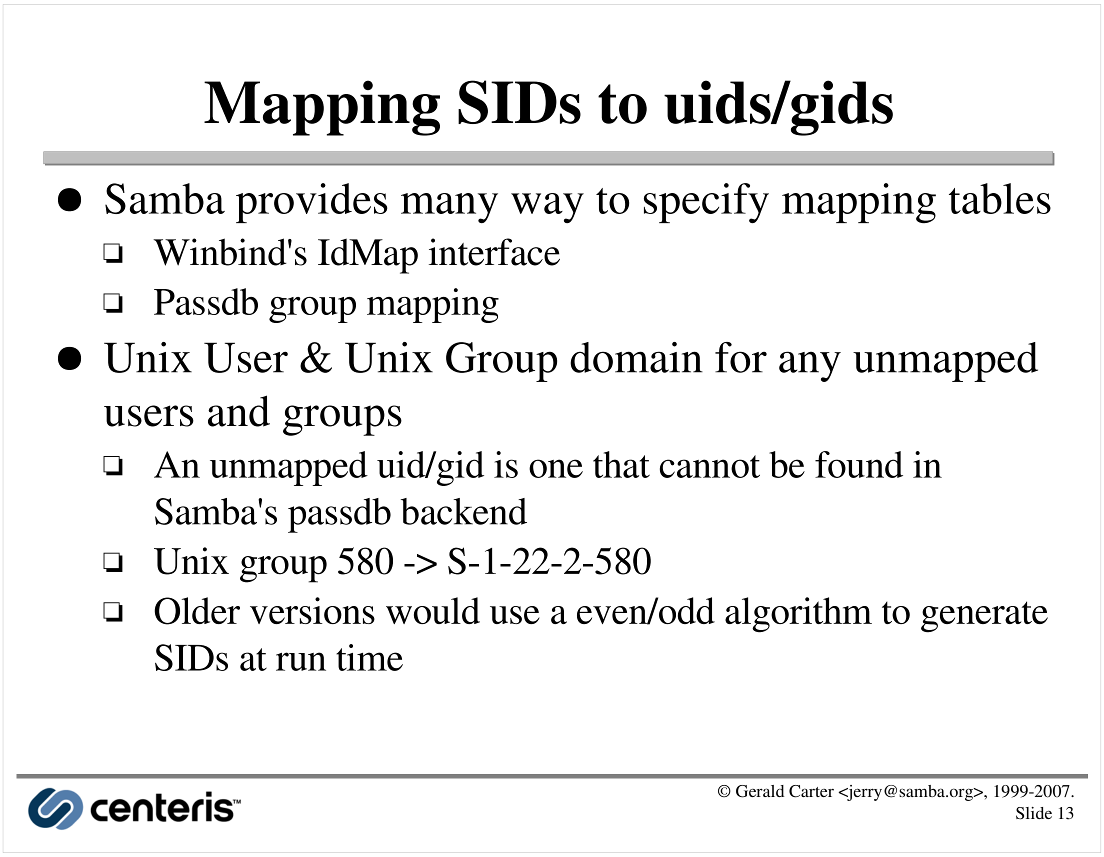
```
NT user token of user S-1-5-21-3234968684-14787312-
   124015166-3136
contains 11 SIDs
SID[  0]: S-1-5-21-3234968684-14787312-124015166-3136
SID[  1]: S-1-5-21-3234968684-14787312-124015166-512
SID[  2]: S-1-1-0
SID[  3]: S-1-5-2
SID[  4]: S-1-5-11
SID[  5]: S-1-5-21-3234968684-14787312-124015166-3125
SID[  6]: S-1-5-21-3234968684-14787312-124015166-3120
SID[  7]: S-1-5-21-3234968684-14787312-124015166-513
SID[  8]: S-1-5-21-3234968684-14787312-124015166-519
SID[  9]: S-1-5-21-3234968684-14787312-124015166-518
SID[ 10]: S-1-5-32-544
```

Logfile: Unix token

```
UNIX token of user 100025
Primary group is 100000 and contains 5 supplementary groups
Group[   0]: 100002
Group[   1]: 100001
Group[   2]: 100003
Group[   3]: 100000
Group[   4]: 60011
```

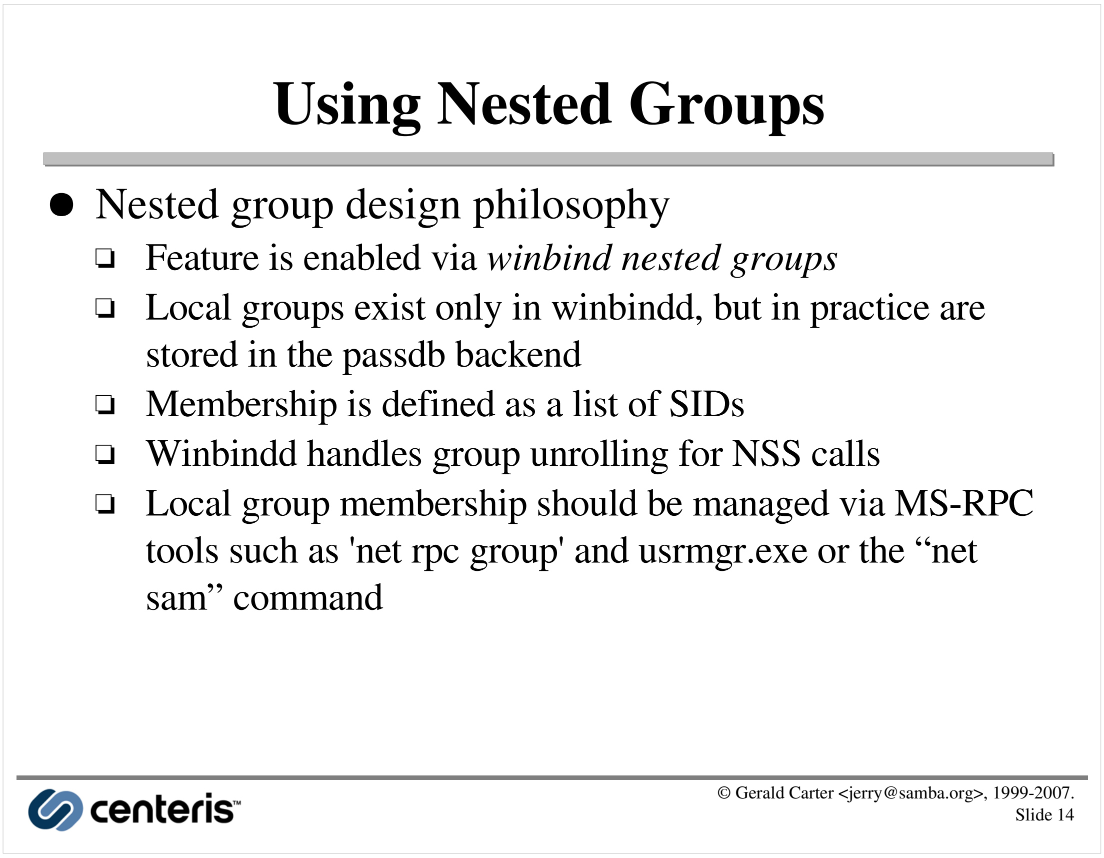
NT token -> Unix token

- Any SID not mapped to a uid/gid is ignored when creating the Unix token
- A Unix token must have a uid and primary gid to be considered valid
- If a valid Unix token cannot be created, the user will be rejected
  - ❑ Not always true; see “map to guest” in smb.conf(5)



Mapping SIDs to uids/gids

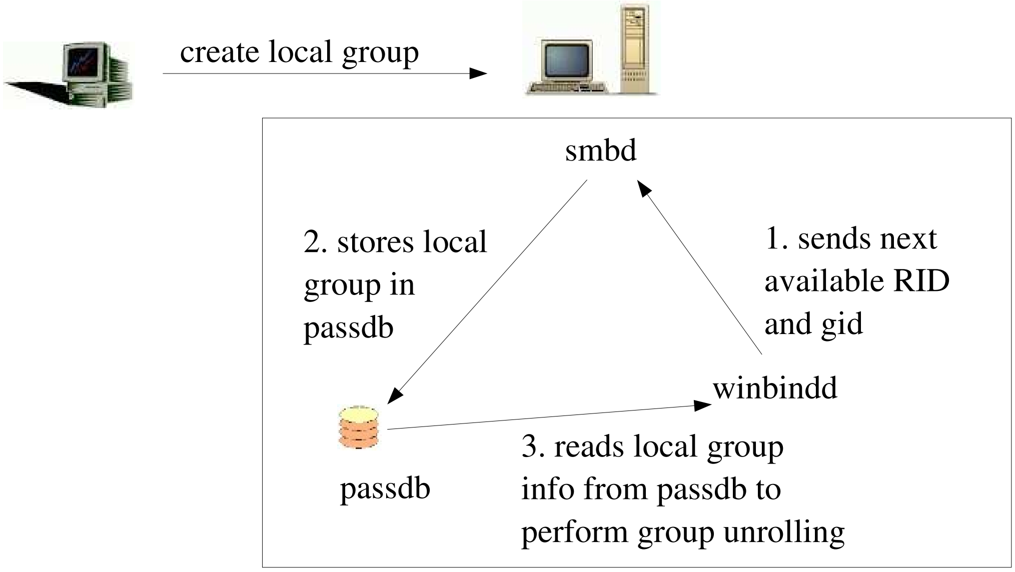
- Samba provides many way to specify mapping tables
  - ❑ Winbind's IdMap interface
  - ❑ Passdb group mapping
- Unix User & Unix Group domain for any unmapped users and groups
  - ❑ An unmapped uid/gid is one that cannot be found in Samba's passdb backend
  - ❑ Unix group 580 -> S-1-22-2-580
  - ❑ Older versions would use a even/odd algorithm to generate SIDs at run time



Using Nested Groups

- Nested group design philosophy
  - ❑ Feature is enabled via *winbind nested groups*
  - ❑ Local groups exist only in winbindd, but in practice are stored in the passdb backend
  - ❑ Membership is defined as a list of SIDs
  - ❑ Winbindd handles group unrolling for NSS calls
  - ❑ Local group membership should be managed via MS-RPC tools such as 'net rpc group' and usrmgr.exe or the “net sam” command

Nested Group Architecture


create local group
smbd
2. stores local group in passdb
1. sends next available RID and gid
winbindd
passdb
3. reads local group info from passdb to perform group unrolling

Winbind Parameters

```
[global]
     netbios name        = SNOW
     workgroup           = BOOKS
     realm               = BOOKS.PLAINJOE.ORG
     security            = ads

     ## winbind settings
     idmap uid               = 10000-20000
     idmap gid               = 10000-20000
     winbind nested groups   = yes
```

net sam

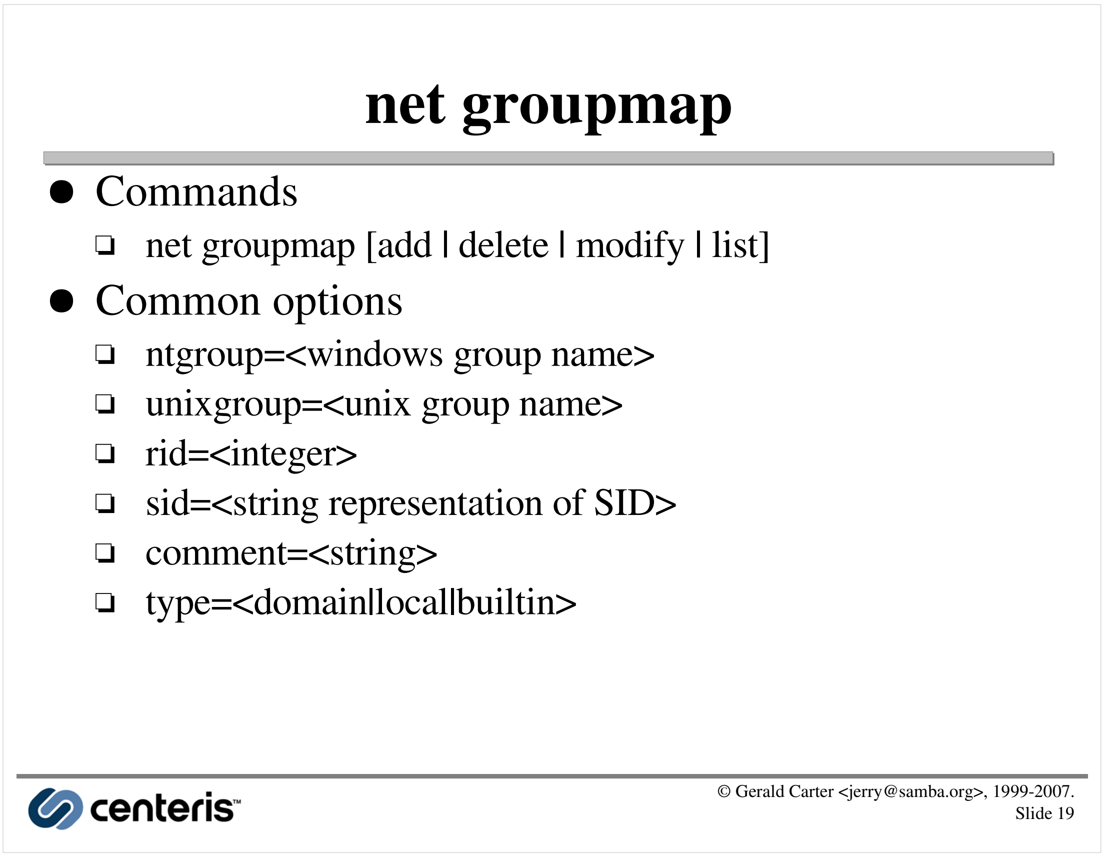
- New replacement for “net groupmap” & pdbedit
- Used to manage BUILTIN and local groups among other things
  - ❑ Local & Builtin groups are stored in the group mapping table and expanded by winbindd
- Example:
  - ❑ net sam createlocalgroup SvnUsers
  - ❑ net sam addmem SvnUsers “DOMAIN\Developers”

net groupmap

- “net groupmap” is a lowlevel database tool for manipulating Samba's group mapping table
  - ❑ Only used for managing domain group mappings
- Only mapped groups will appear in the object picker on clients

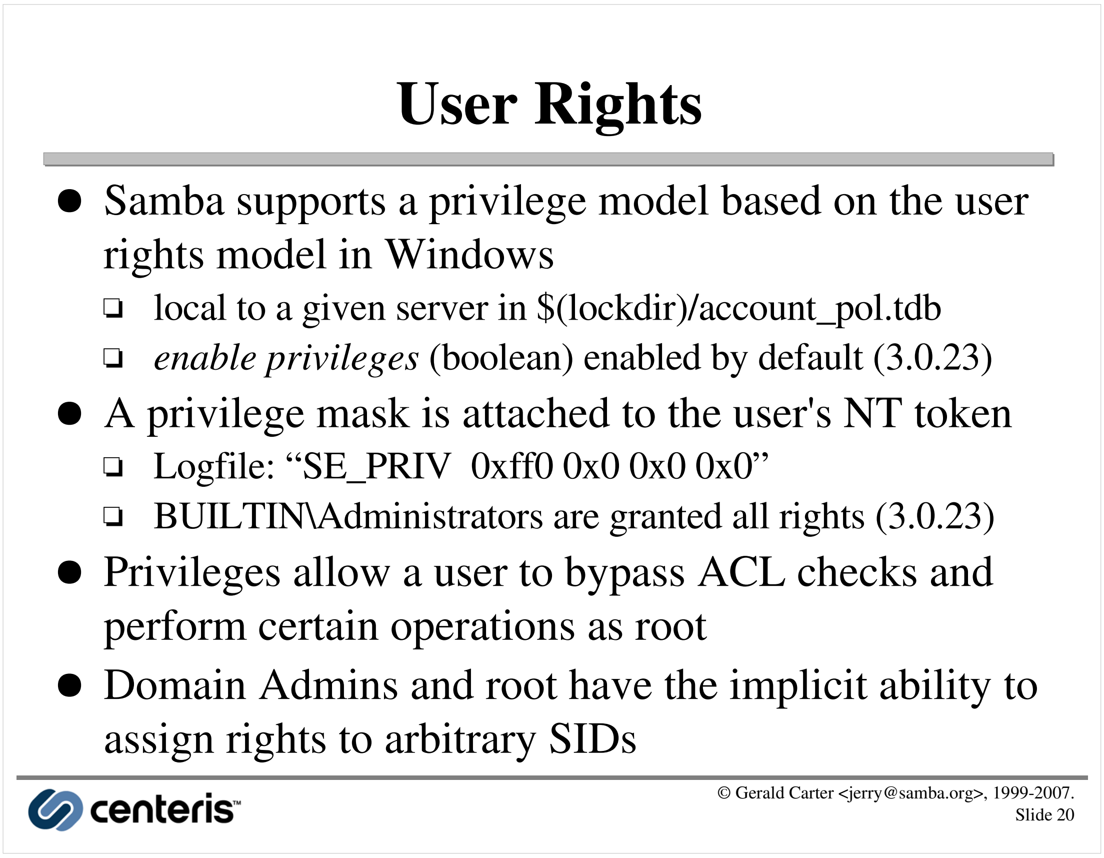
```
root# net groupmap list ntgroup="Domain Admins" verbose

Domain Admins
   SID        : S-1-5-21-2547222302-1596225915-2414751004-512
   Unix group: ntadmin
   Group type: Domain group
   Comment    :
```



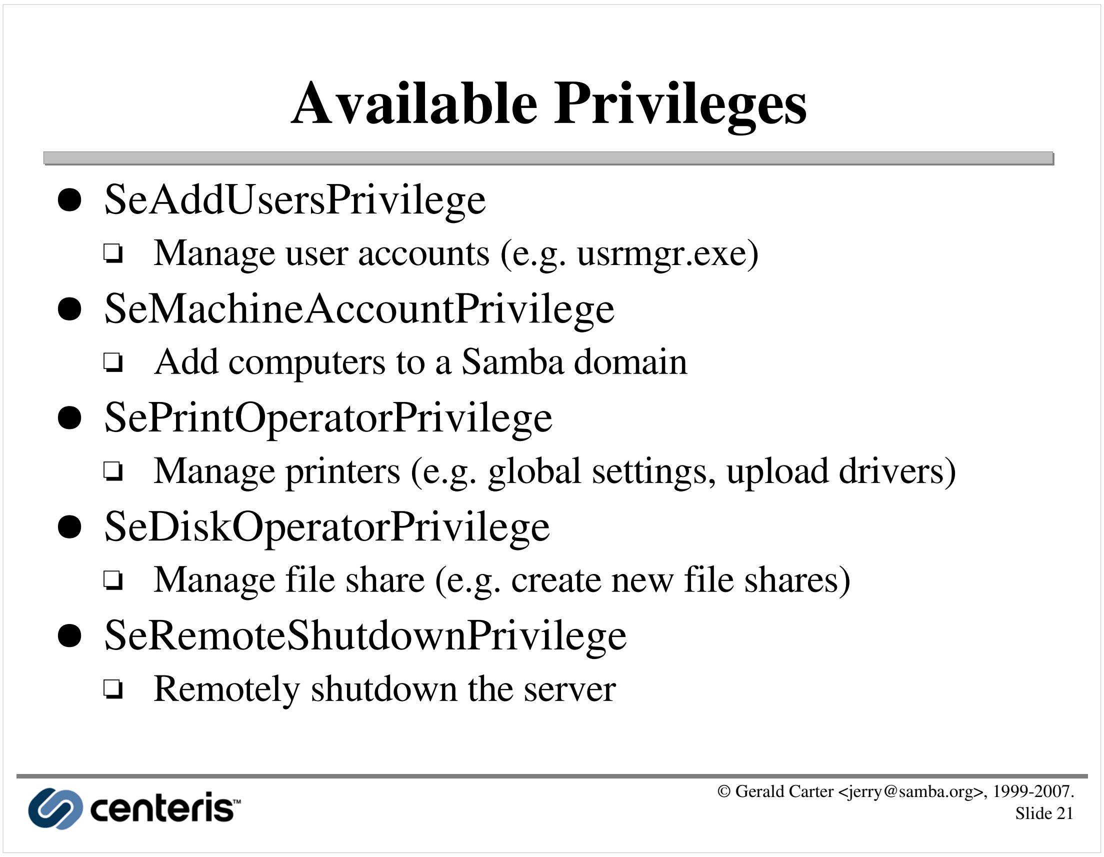
net groupmap

- Commands
  - ❑ net groupmap [add | delete | modify | list]
- Common options
  - ❑ ntgroup=<windows group name>
  - ❑ unixgroup=<unix group name>
  - ❑ rid=<integer>
  - ❑ sid=<string representation of SID>
  - ❑ comment=<string>
  - ❑ type=<domain|local|builtin>



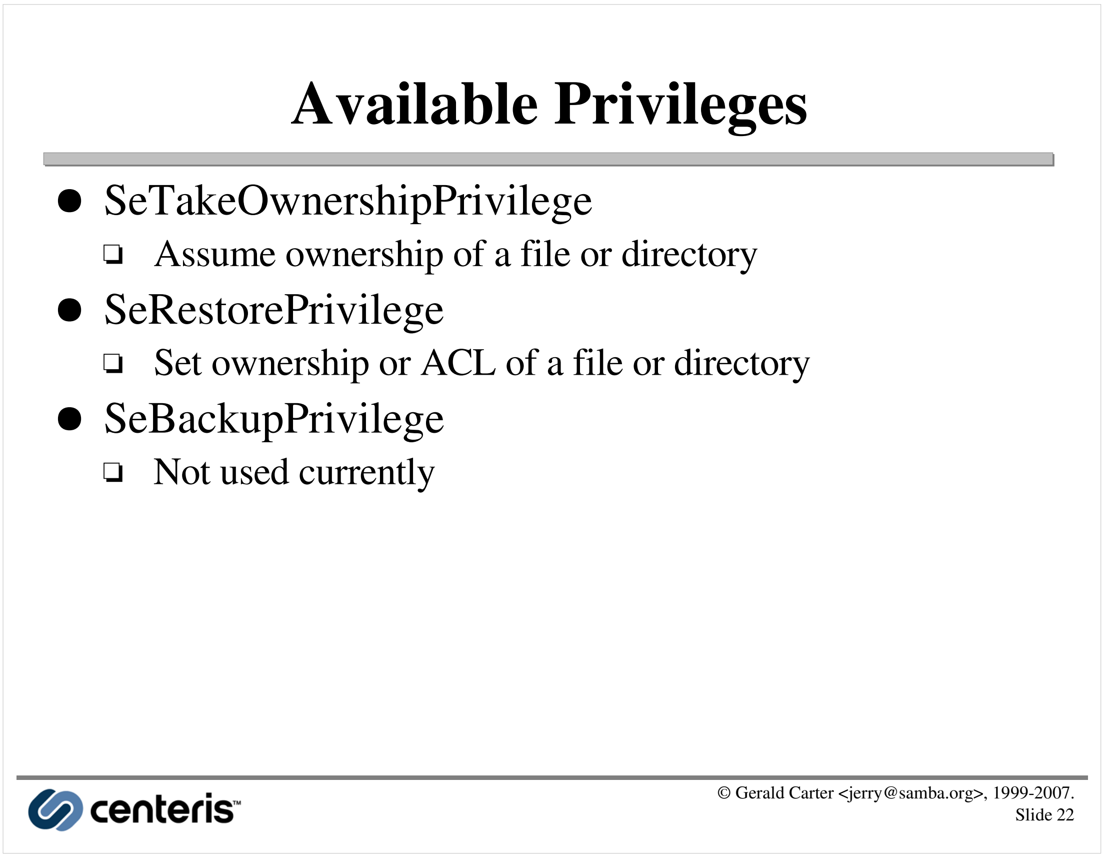
User Rights

- Samba supports a privilege model based on the user rights model in Windows
  - ❑ local to a given server in $(lockdir)/account_pol.tdb
  - ❑ *enable privileges* (boolean) enabled by default (3.0.23)
- A privilege mask is attached to the user's NT token
  - ❑ Logfile: “SE_PRIV 0xff0 0x0 0x0 0x0”
  - ❑ BUILTIN\Administrators are granted all rights (3.0.23)
- Privileges allow a user to bypass ACL checks and perform certain operations as root
- Domain Admins and root have the implicit ability to assign rights to arbitrary SIDs



Available Privileges

- SeAddUsersPrivilege
  - ❑ Manage user accounts (e.g. usrmgr.exe)
- SeMachineAccountPrivilege
  - ❑ Add computers to a Samba domain
- SePrintOperatorPrivilege
  - ❑ Manage printers (e.g. global settings, upload drivers)
- SeDiskOperatorPrivilege
  - ❑ Manage file share (e.g. create new file shares)
- SeRemoteShutdownPrivilege
  - ❑ Remotely shutdown the server



Available Privileges

- SeTakeOwnershipPrivilege
  - ❑ Assume ownership of a file or directory
- SeRestorePrivilege
  - ❑ Set ownership or ACL of a file or directory
- SeBackupPrivilege
  - ❑ Not used currently

Setting up a Print Manager Group

```
root# net getlocalsid VALE
SID for domain VALE is:
   S-1-5-21-2547222302-1596225915-2414751004

root# net groupmap add unixgroup=ntadmins \
  ntgroup=”Domain Admins” \
  sid=S-1-5-21-2547222302-1596225915-2414751004-512
root# net groupmap add unixgroup=printops \
  ntgroup=”Print Admins”
...............
$ id
uid=780(jerry) gid=100(users) groups=100(users),3(sys),
1001(sysadmin),1007(ntadmin),1008(ntusers),1042(printops)

$ net -S queso -U jerry -W VALE rpc rights grant \
  'VALE\Print Admins' SePrintOperatorPrivilege
```

Debugging FAQ: Basic smb.conf

```
## /etc/samba/smb.conf
[global]
      include = /etc/samba/debug.conf
      ...
```

```
## /etc/samba/debug.conf
[global]
      log level = 10
      log file = /var/log/samba/log.%m
      max log size = 0
      debug timestamp = yes
      debug pid = yes
```

Common Grep Expressions

- grep panic log.*
  - ❑ Look for crashes
- grep -E '(WERR_|NT_STATUS)' log.* | grep -v OK
  - ❑ Look for ACCESS_DENIED, etc...
- grep “api_rpcTNP.*unknown$” log.*
  - ❑ Look for unknown MS-RPC calls
- grep DCERPC_FAULT_OP_RNG_ERROR log.*
  - ❑ Misparsed MS-RPC calls

Common Win32 Error Msgs

- Samba does not always send back an appropriate error code
- “A device attached to the system is not functioning”
  - ❑ NT_STATUS_UNSUCCESSFUL
- “No such user”
  - ❑ Machine account creation failed when joining a domain

This page intentionally left blank

This page intentionally left blank

Outline

- Background
  - ❏ Windows SIDs, Local Groups, Group Mapping, User Rights
  - ❏ Debugging FAQ
- Users & Groups
- File & Print Services
  - ❏ Disk Share Management, POSIX ACLs, xcopy /o
  - ❏ Printers, Drivers, Settings
- Monitoring & Management
  - ❏ EventLogs, Service Control, Performance Monitor

Users & Groups

- Supporting the User Manager for Domains has been an ongoing battle
  - ❏ Applies to lusrmgr.msc MMC plugin as well
- External commands for managing Unix/Linux accounts attributes
- Design philosophy
  - ❏ Samba's passdb maintains Windows attributes for existing Unix accounts
  - ❏ Group mapping matches a SID with a Unix/Linux group
  - ❏ Group membership is managed via the Unix/Linux system database (e.g. /etc/passwd and /etc/group)

Passdb Recommendations

- smbpasswd file
  - ❑ Standalone server with no remote management support and no group mapping
  - ❑ Domain member server utilizing on only domain accounts
- tdbsam
  - ❑ Any server utilizing winbind nested groups or remote user management
- ldapsam
  - ❑ Samba Domain Controllers utilizing a shared passdb backend

User/Group Scripts

- Add and remove users
  - ❑ *add user script, delete user script*
  - ❑ *rename user script*
  - ❑ *add machine script*
- Create and remove domain groups
  - ❑ *add group script, delete group script*
- Manage domain group membership
  - ❑ *add user to group script*
  - ❑ *delete user from group script*
  - ❑ *set primary group script*

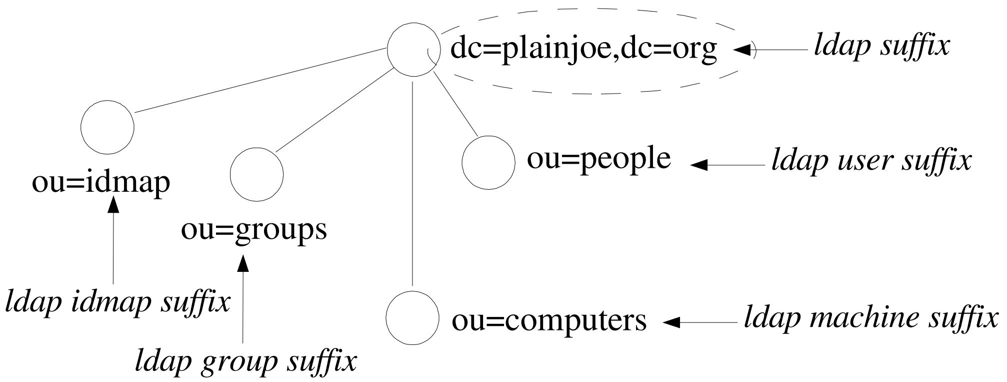
Example Add User Script

```
[global]
  ....
  add user script = /usr/sbin/useradd -m -d /home/%u '%u'
  delete user script = /usr/sbin/userdel -r '%u'
  add group script = /usr/sbin/groupadd -r '%g'
  delete group script = /usr/sbin/groupdel '%g'
  add user to group script = /usr/bin/groupmod -A '%u' '%g'
  delete user from group script = /usr/bin/groupmod \
      -D '%u' '%g'
  set primary group script = /usr/sbin/usermod -g '%g' '%u'
  add machine script = /usr/sbin/useradd -g hosts \
      -c "Samba Machine Account" -m -d /home/%u \
      -s /bin/false %u
```

ldapsam

- OpenLDAP 2.x schema file (samba.schema)
  - ❑ sambaSamAccount contains information useful to smbd
- Samba queries the OS via getpwnam() for uid
  - ❑ Samba does not require the existence of a posixAccount entry for the user
- Additional LDAP directory integration
  - ❑ ldapsam:trusted = yes
  - ❑ ldapsam:editposix = yes

Samba's LDAP DIT



dc=plainjoe,dc=org ← *ldap suffix*

ou=idmap ← *ldap idmap suffix*

ou=groups ← *ldap group suffix*

ou=people ← *ldap user suffix*

ou=computers ← *ldap machine suffix*

ldapsam Parameters

- *ldapsam[_compat]*
  - ❑ ldapsam:ldap[s]://server/
- *ldap admin dn*
  - ❑ use "smbpasswd -w *pass*" to set admin dn password (stored in secrets.tdb)
- *ldap ssl* = [off | start_tls]
- *ldap suffix*
  - ❑ *ldap user suffix*
  - ❑ *ldap machine suffix*
  - ❑ *ldap group suffix*
  - ❑ *ldap idmap suffix*

objectclass: sambaSamAccount

- AUXILARY class
- schema files also exists for
  - ❑ OpenLDAP 2.x
  - ❑ Netscape/SunOne
  - ❑ Novell eDirectory
- *ldapsam_compat* uses the Samba 2.2 objectclass 'sambaAccount' instead

objectClass: sambaSamAccount

uid:
sambaSid:

cn:
sambaPwdLastSet:
sambaLogonTime:
sambaLogoffTime:
sambaKickoffTime:
sambaUserWorkstations:
sambaLMPassword:
sambaNTPassword:
description:
sambaDomainName:
sambaBadPasswordCount:
sambaBadPasswordTime:

sambaPwdCanChange:
sambaPwdMustChange:
sambaAcctFlags:
displayName:
sambaHomePath:
sambaHomeDrive:
sambaLogonScript:
sambaProfilePath:
sambaPrimaryGroupSID:
sambaPasswordHistory:
sambaLogonHours:

Still requires separate password hashes to support NTLM (*ldap password sync*)

objectclass: sambaGroupMapping

- Used to map UNIX groups to SIDs
- Assumes the existence of a rfc2307 posixGroup entry
- *ldap group suffix* (RDN)

objectClass: sambaGroupMapping

gidNumber:
sambaGroupType:
sambaSID:

displayName:
description:

ldapsam:trusted = yes

- Allows smbd to bypass NSS for several query intensive operations
  - ❑ Enumerate members of a group
  - ❑ Retrieve a user's group memberships
  - ❑ SID/name translation
  - ❑ SID/uid/gid translation
- Does not remove the need for installing nss_ldap to handle normal getpwnam() calls performed by smbd

ldapsam:editposix = yes

- The newly added (3.0.25) editposix option provides an alternative to the script based user/group management functions when using an LDAP directory service
- Makes use of the RFC 2307 schema object classes and attributes
- Uses the same ldap search suffixes from smb.conf

Debugging User Mgt Scripts

- Determine which side of the user management is failing
- Process for adding a new user
  - Client issues SamrCreateUser() call
  - smbd checks for SeAddUserPrivilege in NT user token and switches to uid 0 if found
  - If Unix user does not exist, smbd invokes the “add user script”
    - Performed as the connected user if privilege check failed
  - Did “add user script” succeed ? Yes – Add to passdb backend

centeris™

Debugging User Mgt Scripts

- smbd records the exist code of the “add user script” in logfile
  - In general, 0 indicates success
- If the script failed, try running it by hand or possible pipe output to a log file
  - Make sure that the connected user can write to the log file
- Suggestion: Debug the scripts outside of smbd first before testing from a Windows client
  - Scripts should only manipulate Unix attributes

centeris™

This page intentionally left blank

This page intentionally left blank

Outline

- Background
  - Windows SIDs, Local Groups, Group Mapping, User Rights
  - Debugging FAQ
- Users & Groups
- File & Print Services
  - Disk Share Management, POSIX ACLs, xcopy /o
  - Printers, Drivers, Settings
- Monitoring & Management
  - EventLogs, Service Control, Performance Monitor

Windows Equivalent smb.conf

```
[global]
    enable asu support = no
    ...
[c$]
    path = /data/smb/c

[admin$]
    path = /data/smb/c/windows

[print$]
    path = /data/smb/c/windows/system32/spool/drivers
```

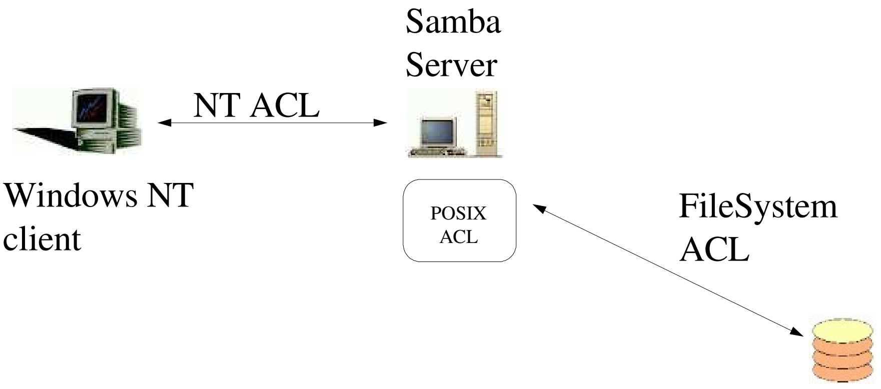
File Services

- File shares
  - Create share directory tree and shares in smb.conf
  - Migrating files/directories
- DOS Attribute Bits
  - Extended attribute support
  - ReadOnly, System, Hidden, Archive
- Access Control Lists
  - Migrating permissions
  - Interpreting Posix ACL support

Filesystem ACLs

- Support for filesystem ACLs is detected at compile time
  - ./configure --with-acl-support
  - Attempts to locate support for EAs (Linux and some *BSDs)
  - POSIX ACLs (Linux ext2/3), XFS (Linux and IRIX), ReiserFS, Solaris, HP-UX, etc...
  - Run `smbd -b | grep ACL` to verify support
- Separate from file share ACLs
  - ${lockdir}/share_info.tdb
- Linux servers should have the following packages
  - libacl, libacl-devel, libattr, libattr-devel

Handling Windows ACLs



Samba Server

NT ACL

Windows NT client

POSIX ACL

FileSystem ACL

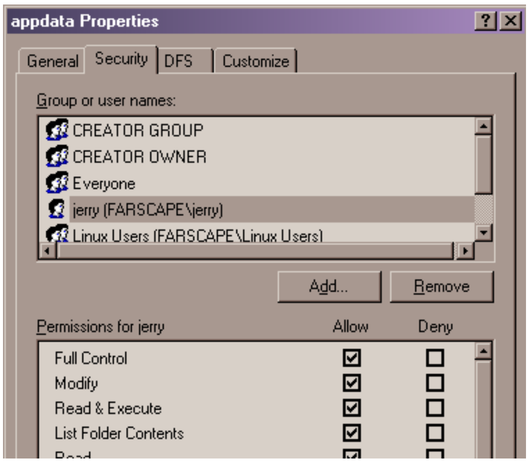
POSIX ACLs Semantics

- No new permission bits (rwx)
  - ❑ Normal u/g/o
    - ✔ [user|group|other]::<perms>
  - ❑ Named users and groups
    - ✔ [user|group]:<name>:<perms>
  - ❑ mask::<perms>
    - ✔ Applied to group perms using a logical AND
- Does jsmith have permissions to this file?
  - ❑ Explicit entries match first
  - ❑ Sum of group perms otherwise
- Default ACLs on directories are inherited

Interpreting Samba ACLs

- Security tab may not display permissions
  - ❑ Permissions on directories must apply to folders, subfolders, & files in order to show up
  - ❑ Permissions on files always show up
- Directories possess additional entries when default ACLs are present
  - ❑ CREATOR {OWNER,GROUP} match the default ACE for the directory owner and group

Interpreting Samba ACLs



appdata Properties

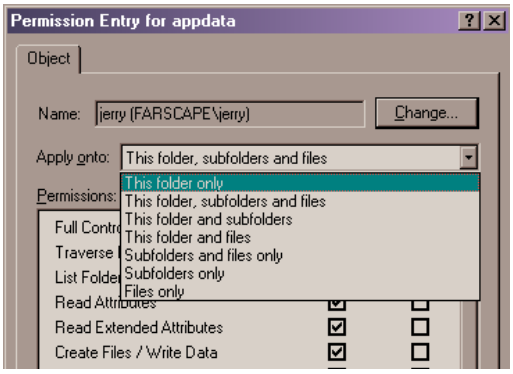
General | Security | DFS | Customize

Group or user names:

- CREATOR GROUP
- CREATOR OWNER
- Everyone
- jerry (FARSCAPE\jerry)
- Linux Users (FARSCAPE\Linux Users)

Add... Remove

Permissions for jerry	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□



Permission Entry for appdata

Object

Name: jerry (FARSCAPE\jerry) Change...

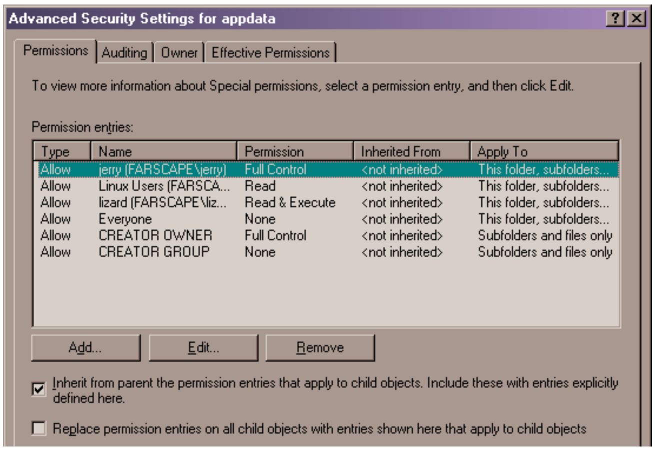
Apply onto: This folder, subfolders and files

- This folder only
- This folder, subfolders and files
- This folder and subfolders
- This folder and files
- Subfolders and files only
- Subfolders only
- Files only

Permissions:	Allow	Deny
Full Contr		
Traverse		
List Folde		
Read Attributes	☑	□
Read Extended Attributes	☑	□
Create Files / Write Data	☑	□

Interpreting Samba ACLs

```
$ getfacl appdata
# file: appdata
# owner: jerry
# group: users
user::rwx
user:lizard:r-x
group::r--
mask::rwx
other::---
default:user::rwx
default:user:jerry:rwx
default:user:lizard:r-x
default:group::---
default:group:users:r--
default:mask::rwx
default:other::---
```



To view more information about Special permissions, select a permission entry, and then click Edit.

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	jerry (FARSCAPE\jerry)	Full Control	<not inherited>	This folder, subfolders...
Allow	Linux Users (FARSCA...	Read	<not inherited>	This folder, subfolders...
Allow	lizard (FARSCAPE\liz...	Read & Execute	<not inherited>	This folder, subfolders...
Allow	Everyone	None	<not inherited>	This folder, subfolders...
Allow	CREATOR OWNER	Full Control	<not inherited>	Subfolders and files only
Allow	CREATOR GROUP	None	<not inherited>	Subfolders and files only

☑ Inherit from parent the permission entries that apply to child objects. Include these with entries explicitly defined here.

☐ Replace permission entries on all child objects with entries shown here that apply to child objects

ACL Parameters

- *nt acl support* (boolean)
  - Should the share report ACL support to clients?
- *map acl inherit* (boolean)
  - Should the acl inherited bit be stored as an EA for a directory?
- *inherit acls* (boolean)
  - Should default acls on directories be propagated?
- *acl map full control* (boolean)
  - Should "rwx" be reported as "Full Control"?

ACL Parameters

- *dos filemode* (boolean)
  - Implement windows semantics to modify timestamps, owner, and permissions
- *profile acls* (boolean)
  - Report the owner of all files in a share as the Administrators group SID
  - Work around for policy setting in Windows AD domains

DOS Attributes

- Matter much more than you would think
  - Registry hives (e.g. ntuser.dat, ntconfig.pol) will not load if marked as ReadOnly
- Historically have been represent with the 'x' permission bits
- *store dos attributes* (boolean)
  - Store attribute settings in a file or directory's EA

Recommended File Settings

- Linux appears to have the best support for ACLs and EAs required by Samba
- Ensure smbd was built with ACLs

```
[global]
    ...
    store dos attributes = yes
    inherit acls         = yes
    map acl inherit      = yes
    nt acl support       = yes
    read only            = no
```

Managing Shares

- Example scripts for managing shares
  - ❑ samba/examples/scripts/shares
- *add share command*, *change share command* (string)
  - ❑ Absolute path to smb.conf
  - ❑ Share name
  - ❑ Absolute path to be shared
  - ❑ Comment
  - ❑ Max connections
- *delete share command* (string)
  - ❑ Absolute path to smb.conf
  - ❑ Share name

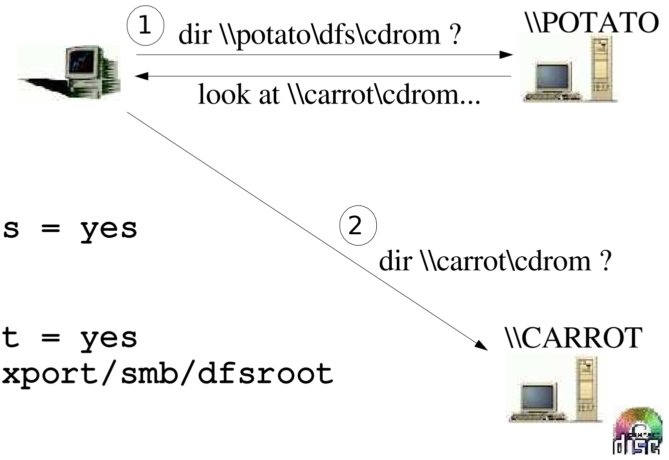
Migrating File Shares

- Can manage shares via
  - Windows MMC
  - Editing smb.conf
  - *net rpc share*
- net rpc share migrate {shares,files,security,all}
  - Migrate settings from a remote server to the local Samba host
  - Requires admin rights on remote and local servers
- Windows tools such as "xcopy /o" and "robocopy" can also be used for copy file permissions
- Beware of files owner by groups

MS Distributed File System

- MS-DFS can help to ease file share migration by insulating users from the actual location of data
- Not the same thing as DCE/DFS
- Native client support in all modern Windows releases

MS DFS - A Graphic



```
[global]
     host msdfs = yes
     .....
[dfs]
     msdfs root = yes
     path = /export/smb/dfsroot
```

MS DFS Parameters

- *host msdfs* (boolean) (G)
  - ❑ Should smbd act as a MS-DFS server?
- *msdfs root* (boolean) (S)
  - ❑ Does this service contain MS-DFS redirects?
  - ❑ msdfs links can coexist with local files/directories

```
# ln -s msdfs:server\\share[,server\\share] directory
( e.g. cdrom -> msdfs:queso\cdrom)
```

- *msdfs proxy* (string) (S)
  - ❑ UNC path to share containing the real MS-DFS referrals
  - ❑ e.g. \\server1\share refers to \\server2\share

Print Services

- Print queues
  - ❑ Create the necessary CUPS print queues
- Print shares
  - ❑ Create the shares in smb.conf
- Print drivers
  - ❑ Migrate driver files and metadata
- Printer settings
  - ❑ Duplex settings, paper trays, etc....

Printers in Samba

- Print queues exist outside of Samba
  - ❑ e.g. CUPS or LPRng queues
- Print shares exist in smb.conf
- Print drivers are defined in ${lockdir}/ntdrivers.tdb with the actual drivers files in [print$]
- Printer objects associate Windows spooler metadata with a print share and are defined in ${lockdir}/ntprinters.tdb
  - ❑ Binding of a driver to a printer object
- Printer migration requires a working Point-n-Print server

Point & Print

- The ability to automatically server printer drivers to Windows clients upon demand
  - ❑ LanMan Printing API
  - ❑ Windows NT and later use RPC based printing
- Create print services in smb.conf as usual
- Printer drivers must be "installed" on the Samba server and bound to printers

Assigning Printer Drivers

- Driver files are stored in [print$]
  - ❑ Hard coded file share name used to store printer drivers
  - ❑ Contains subdirectories for various OS versions
  - ❑ Drivers can be uploaded using
    - ✔ the "New driver..." button on the printer properties page
    - ✔ Drivers tab in the Server Properties window
- Driver information is stored in ${lockdir}/nt*.tdb
- Initialize the DeviceMode
- Permissions to upload drivers are controlled by
  - ❑ Write access to the [print$] share
  - ❑ Access as root or with the SePrintOperatorPrivilege

Ports in Samba

- Samba has one default printer port which is primarily cosmetic (*Samba Printer Port*)
- *enum ports command* (string)
  - ❑ External script to enumerate the available ports
  - ❑ Must print the list to stdout
- *add port command* (string)
  - ❑ New in 3.0.23
  - ❑ Passed two parameters
    - ✔ port name
    - ✔ deviceURI (socket:// or lpd://)
  - ❑ e.g. addport hp2100 socket://hp2100.plainjoe.org:9100/

Creating Printers from Windows

- *add printer command* (string)
  - ❑ Invoked when receiving an {Add,Set}Printer() RPC
  - ❑ Seven parameters
    - ✔ Printer name
    - ✔ Share name
    - ✔ Port name
    - ✔ Driver name
    - ✔ Location
    - ✔ Comment
    - ✔ Remote machine that executed the call
- *delete printer command* (string)
  - ❑ Invoked when receiving an DeletePrinter() RPC
  - ❑ Accepts the share name as a single parameter

Migrating Printers

- Drivers must be migrated first
- net rpc printer migrate
  - ❑ subcommands: all, drivers, printers, forms, settings, security
  - ❑ Requires admin rights on the remote and local server
- Microsoft Print Migrator
  - ❑ http://www.microsoft.com/printserver
  - ❑ Stores printer data and drivers in a single *.cab file
- Both tools work against remote servers

Printmig.exe Requirements

- Must have an [admin$] share on the target server with the same layout as %SYSTEMROOT% on a Windows host
  - ❑ \\foo\admin$\system32\spool\drivers -> \\foo\print$\
- In 3.0.23 a member of the local Administrators group
  - ❑ Required to stop and start the smbd spooler service
- Backups and restores are done primarily through Registry calls and not spooler calls
- The *add printer command* must be able to handle the printer names from the target server

This page intentionally left blank

This page intentionally left blank

Outline

- Background
  - ❑ Windows SIDs, Local Groups, Group Mapping, User Rights
  - ❑ Debugging FAQ
- Users & Groups
- File & Print Services
  - ❑ Disk Share Management, POSIX ACLs, xcopy /o
  - ❑ Printers, Drivers, Settings
- Monitoring & Management
  - ❑ EventLogs, Service Control, Performance Monitor

Eventlogs

- The EventLog API on Windows is a very simple log record retrieval API
- Current Samba design simple reads log records from a tdb file to service the Eventlog MS-RPC requests
- *eventlog list* (list)
  - ❑ List of Eventlog names reported to Clients
  - ❑ $(libdir)/eventlog/<eventlogname>.tdb
  - ❑ The tdb must be populated outside of Samba

Creating an EventLog

- smbd will create an empty eventlog tdb upon receiving an OpenEventLog() call if the file does not exist
- eventlogadm(8)
  - ❑ Add the Eventlog source name and message file to the registry
    - ✔ -o addsource <EventlogName> <sourcename> <msgfileDLLname>
  - ❑ Read and event record from stdin and write it to the tdb
    - ✔ -o write <Eventlog Name>

Message Files

- Described in the Win32 Platform SDK
  - ❑ Resource file
  - ❑ HKLM\SYSTEM\CurrentControlSet\Services\Eventlog
    - ✔ <LogFileName>\<SourceName>
      - ❍ “EventMessageFile = FileName.DLL”
- Downloaded by the client from \c$\windows\system32\ on the server in order to parse EventLogRecords

EventLog Record

- samba/examples/scripts/eventlog/parselog.pl
  - ❑ Generate records from syslog log files

```
LEN: 0
RS1: 1699505740
RCN: 0
TMG: 1128631322
TMW: 1128631322
EID: 1000
ETP: INFO
ECT: 0
RS2: 0
CRN: 0
USL: 0
SRC: cron
SRN: dmlinux
STR: (root) CMD ( rm -f /var/spool/cron/lastrun/cron.hourly)
DAT:
```

Access Control to EventLog Files

- In order to read and EventLog, the client must have read permissions to the tdb
  - ❑ smbd converts the tdb file ACL to a security descriptor and checks against the NT user token
  - ❑ Similar checks for the capability to clear the EventLog
- Viewing Eventlog properties
  - ❑ Clients must be able to access \C$\windows\system32\config\<EventLogName>.evt

Service Control

- Samba can act as a front end to the SysV init script interface
  - ❑ Scripts must support the *stop*, *start*, and *status* commands
- *svcctl list* (list)
  - ❑ Defines list of init script names to be managed
  - ❑ Create links to /etc/init.d/$service in $(libdir)/svcctl
- Four built-in services enabled by default
  - ❑ Net Logon ([netlogon])
  - ❑ Print Spooler (disable spoolss)
  - ❑ Remote Registry Service
  - ❑ WINS (wins support)

Access Control

- By default, services can only be managed by members of the BUILTIN\Administrators group
- Security descriptors can be set on a per service basis using the Windows XP sc.exe command
  - ❑ Uses the Security Descriptor Definition Language (SDDL)
  - ❑ http://msdn2.microsoft.com/en-us/library/aa379567.aspx

net rpc service

- The *net rpc service* command can be used view, stop, and start services on remote Windows and Samba hosts
- Commands: list, start, stop, pause, resume, status
- Due to the use of MS-RPC, obeys same access control as a Windows clients

This page intentionally left blank

Performance Monitoring

- Windows Perfmon.exe simply queries stateless registry values in the HKPD hive
  - ❑ The client records and displays the delta of each query
  - ❑ Current access controls allows read permission for all users
- Samba services these requests based on data stored in $(lockdir)/perfmon/{names,data}.tdb
- These tdbs must be populated from outside of smbd
- Very Linux specific example daemon that reads from /proc included in samba/examples/perfmon/

Perfcount

- Supported counters
  - ❑ CPU usage
  - ❑ Disk usage
  - ❑ Memory Usage
  - ❑ Current runing processes

^D

Gerald (Jerry) Carter
SAMBA Team
Centeris

jerry@samba.org
http://www.samba.org/
http://www.centeris.com/