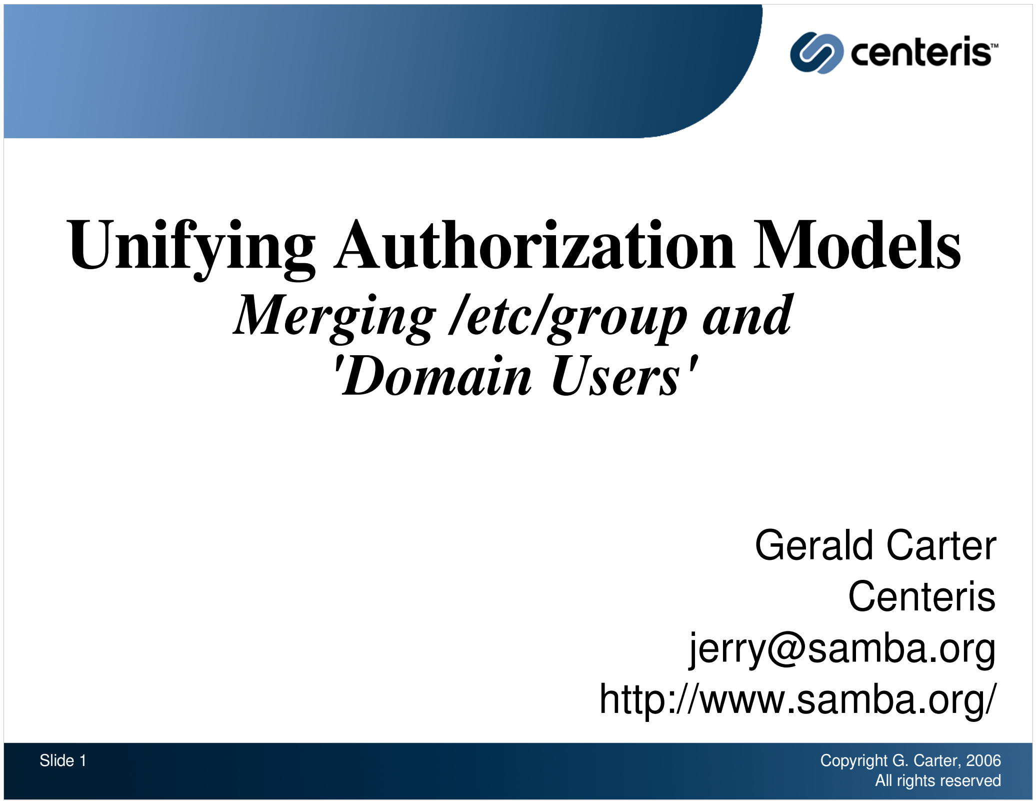
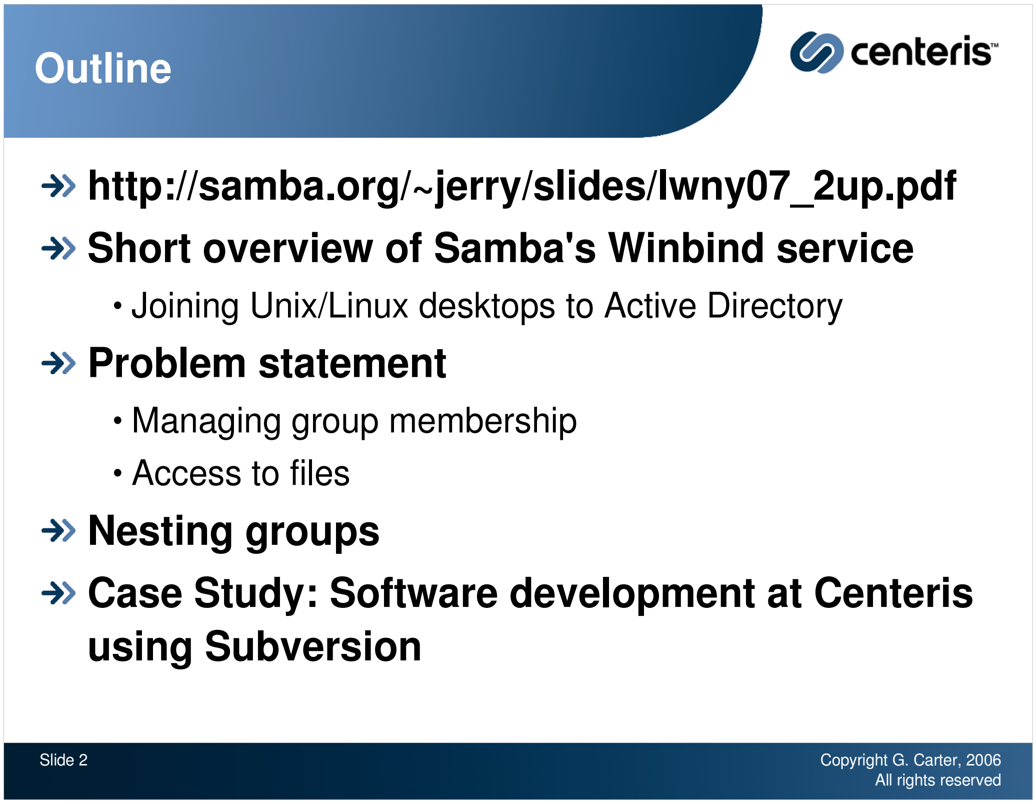


Unifying Authorization Models

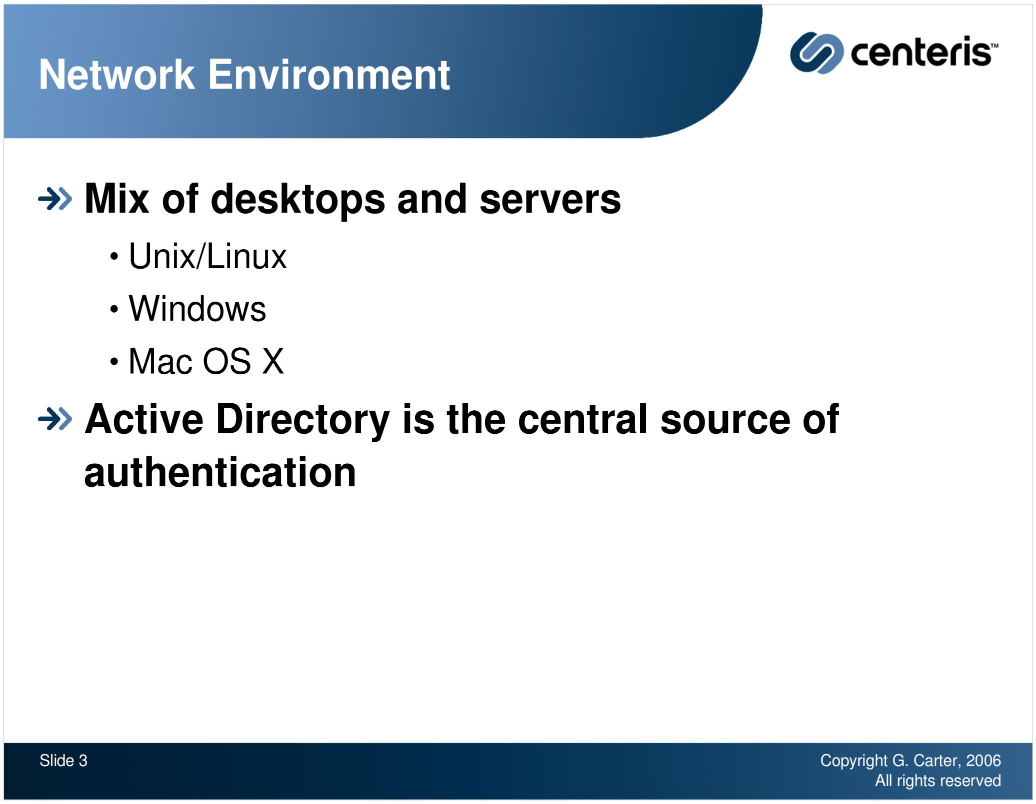
Merging /etc/group and 'Domain Users'

Gerald Carter
Centeris
jerry@samba.org
http://www.samba.org/



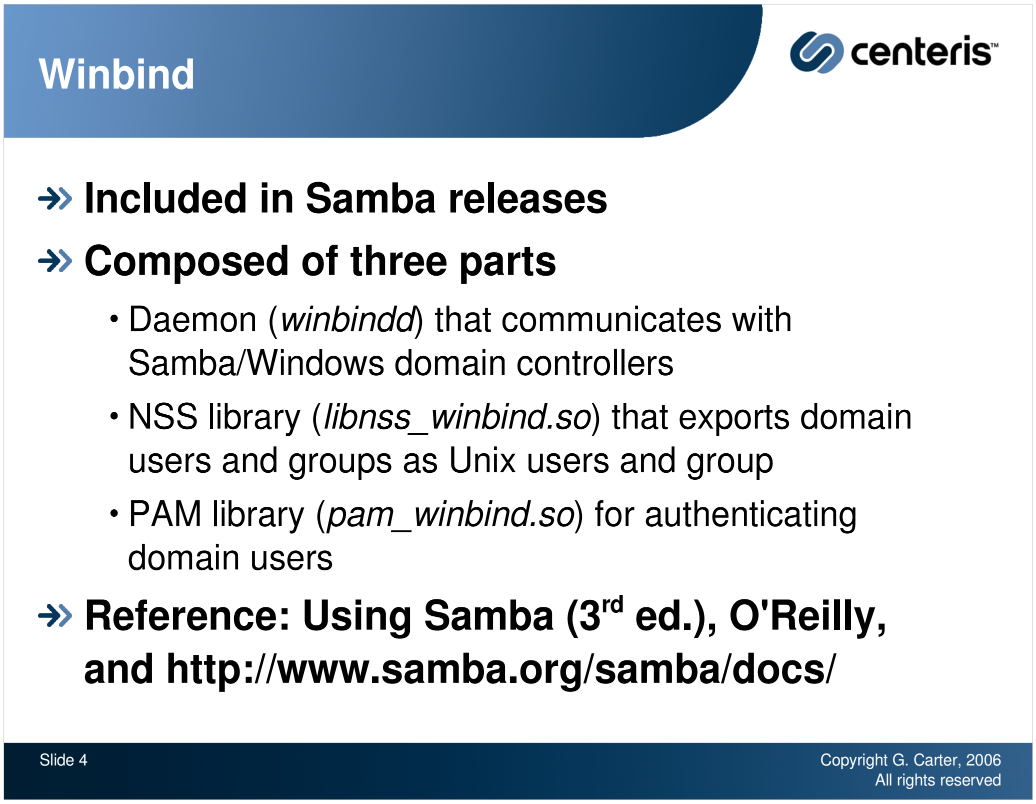
Outline

- http://samba.org/~jerry/slides/lwny07_2up.pdf
- Short overview of Samba's Winbind service
  - Joining Unix/Linux desktops to Active Directory
- Problem statement
  - Managing group membership
  - Access to files
- Nesting groups
- Case Study: Software development at Centeris using Subversion



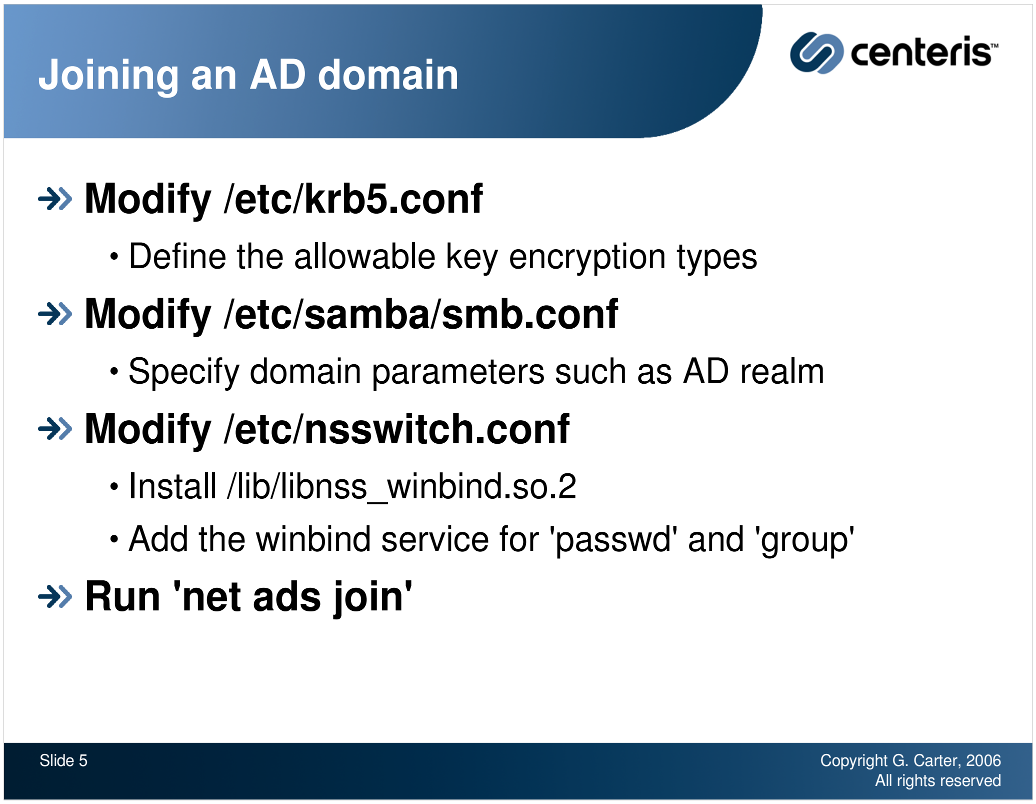
Network Environment

- Mix of desktops and servers
  - Unix/Linux
  - Windows
  - Mac OS X
- Active Directory is the central source of authentication



Winbind

- Included in Samba releases
- Composed of three parts
  - Daemon (*winbindd*) that communicates with Samba/Windows domain controllers
  - NSS library (*libnss_winbind.so*) that exports domain users and groups as Unix users and group
  - PAM library (*pam_winbind.so*) for authenticating domain users
- Reference: Using Samba (3rd ed.), O'Reilly, and http://www.samba.org/samba/docs/

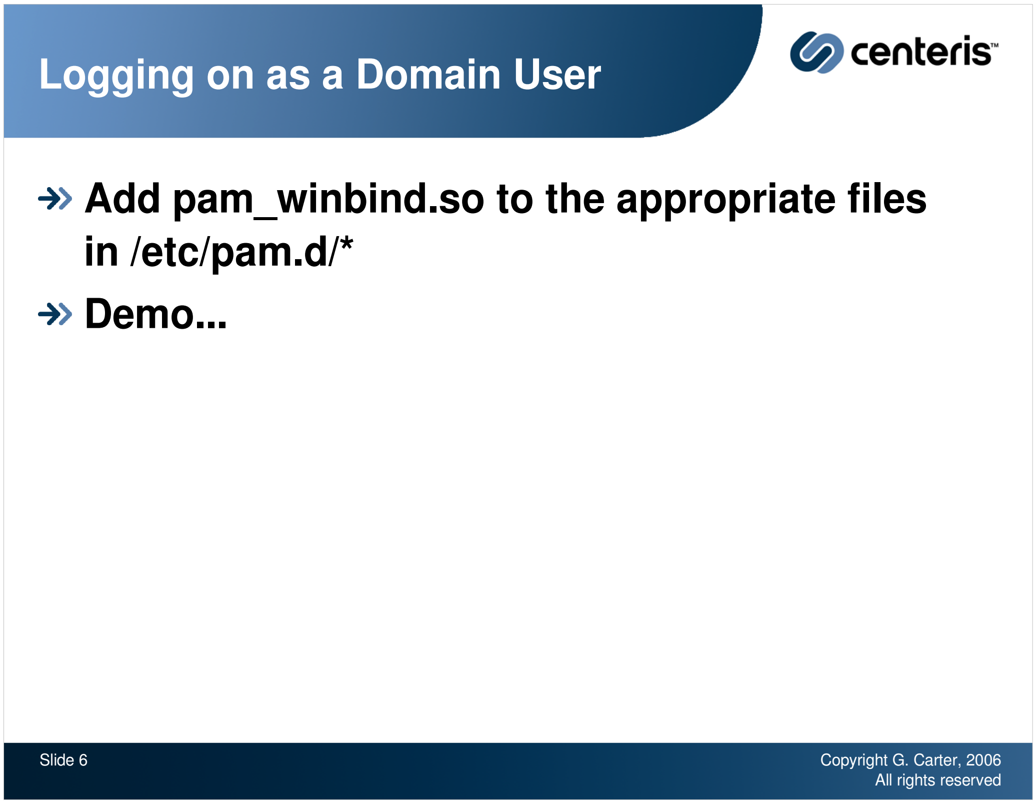


Joining an AD domain

centeris™

- **Modify /etc/krb5.conf**
  - Define the allowable key encryption types
- **Modify /etc/samba/smb.conf**
  - Specify domain parameters such as AD realm
- **Modify /etc/nsswitch.conf**
  - Install /lib/libnss_winbind.so.2
  - Add the winbind service for 'passwd' and 'group'
- **Run 'net ads join'**

Slide 5

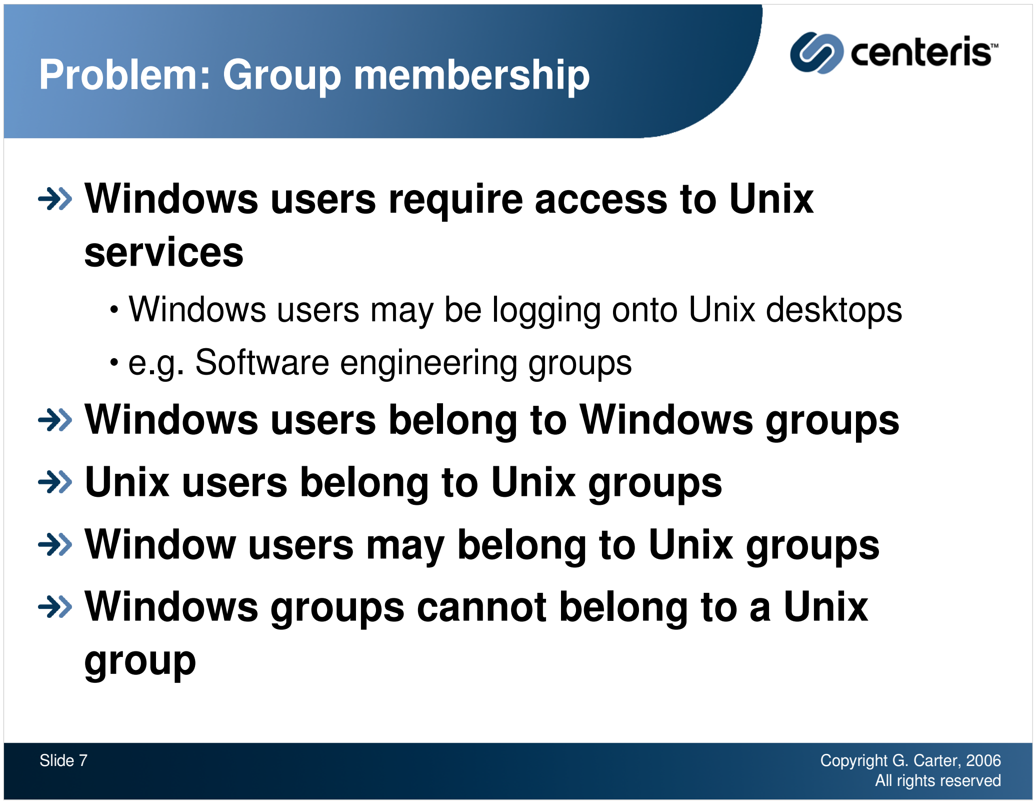


Logging on as a Domain User

centeris™

- **Add pam_winbind.so to the appropriate files in /etc/pam.d/***
- **Demo...**

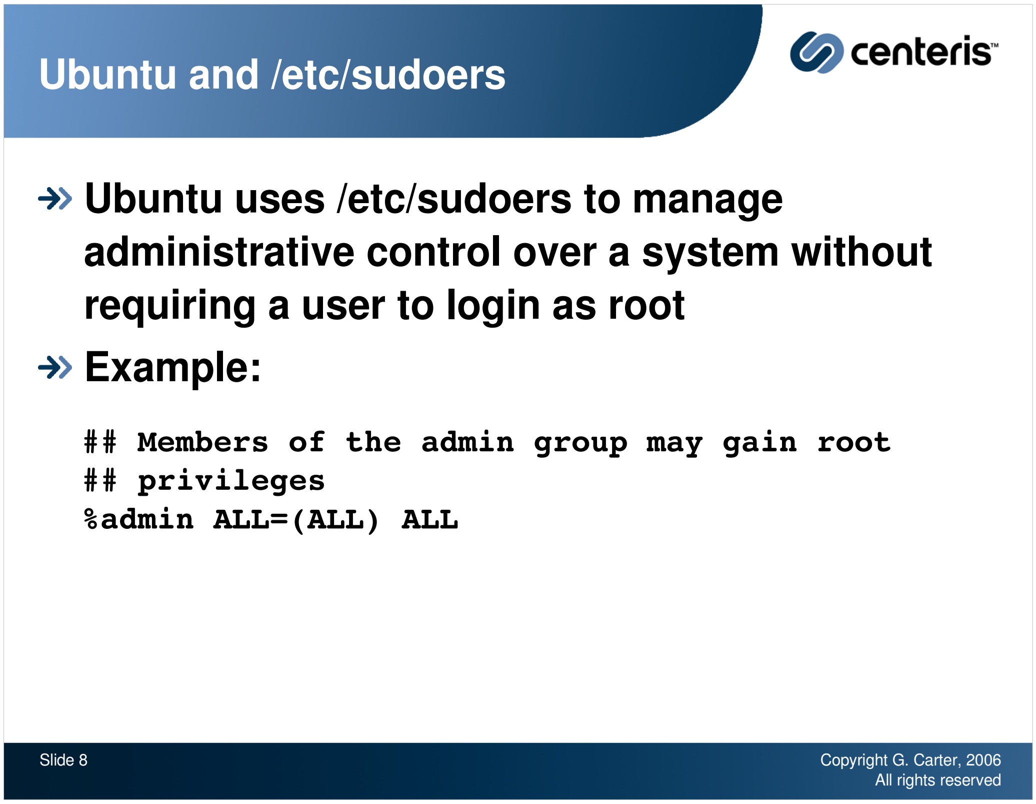
Slide 6



Problem: Group membership

- Windows users require access to Unix services
  - Windows users may be logging onto Unix desktops
  - e.g. Software engineering groups
- Windows users belong to Windows groups
- Unix users belong to Unix groups
- Window users may belong to Unix groups
- Windows groups cannot belong to a Unix group

Slide 7

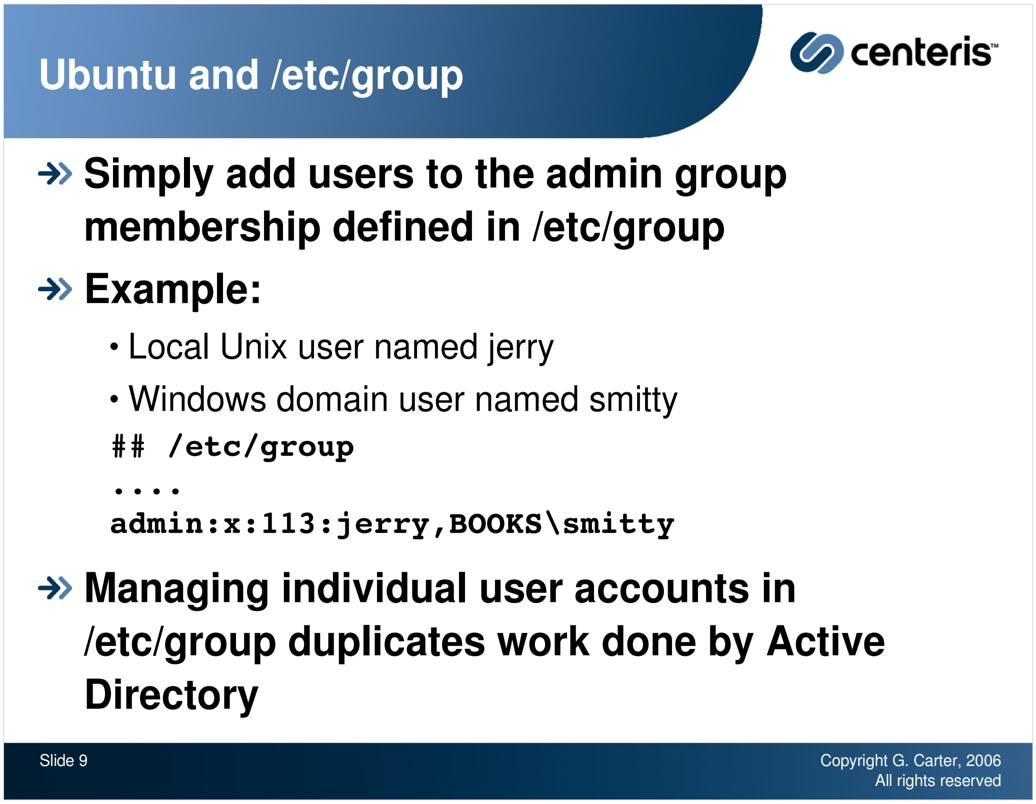


Ubuntu and /etc/sudoers

- Ubuntu uses /etc/sudoers to manage administrative control over a system without requiring a user to login as root
- Example:

```
## Members of the admin group may gain root
## privileges
%admin ALL=(ALL) ALL
```

Slide 8



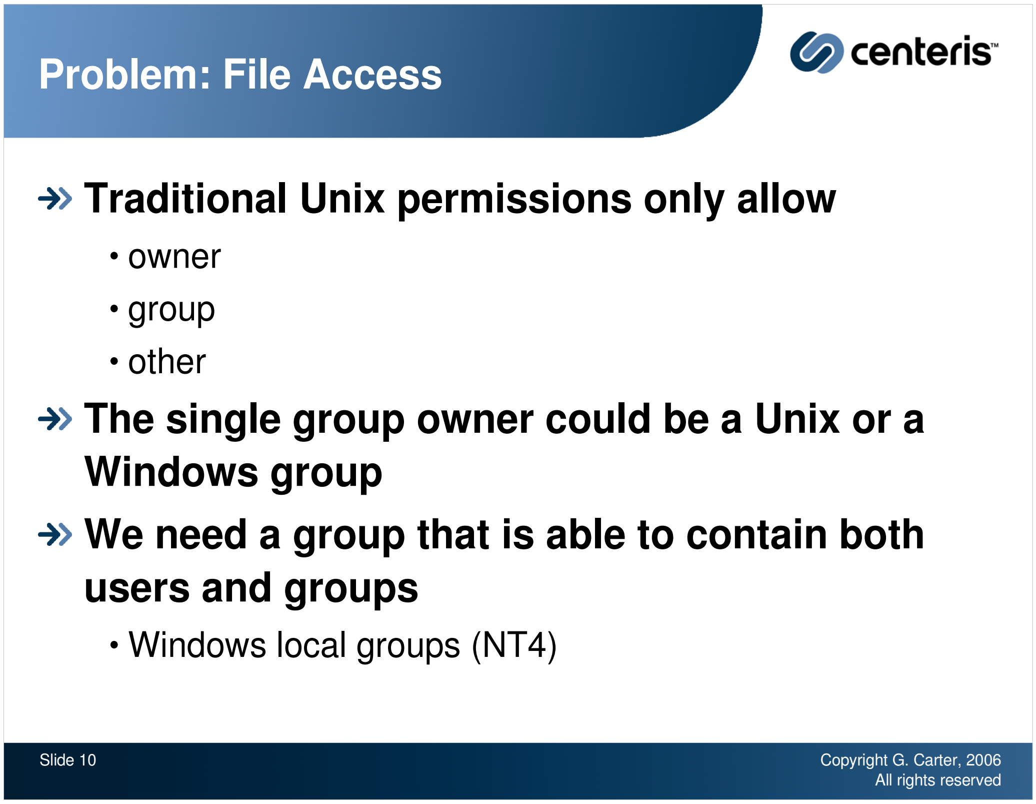
Ubuntu and /etc/group

- Simply add users to the admin group membership defined in /etc/group
- Example:
  - Local Unix user named jerry
  - Windows domain user named smitty

```
## /etc/group
....
admin:x:113:jerry,BOOKS\smitty
```

- Managing individual user accounts in /etc/group duplicates work done by Active Directory

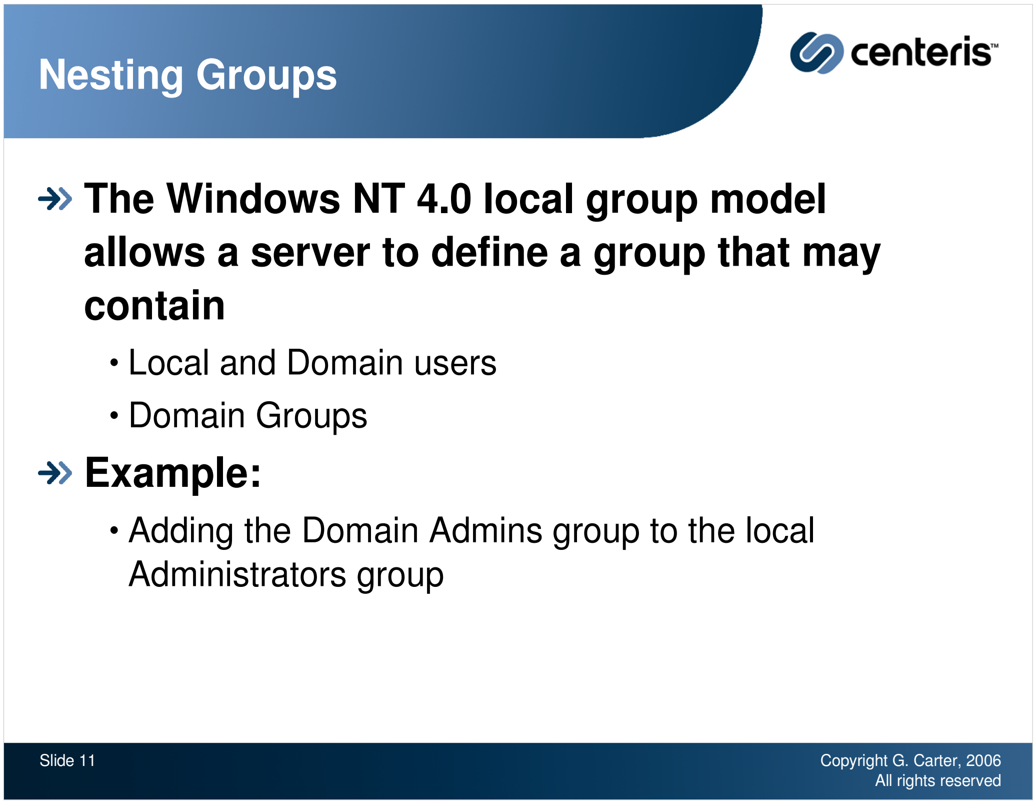
Slide 9



Problem: File Access

- Traditional Unix permissions only allow
  - owner
  - group
  - other
- The single group owner could be a Unix or a Windows group
- We need a group that is able to contain both users and groups
  - Windows local groups (NT4)

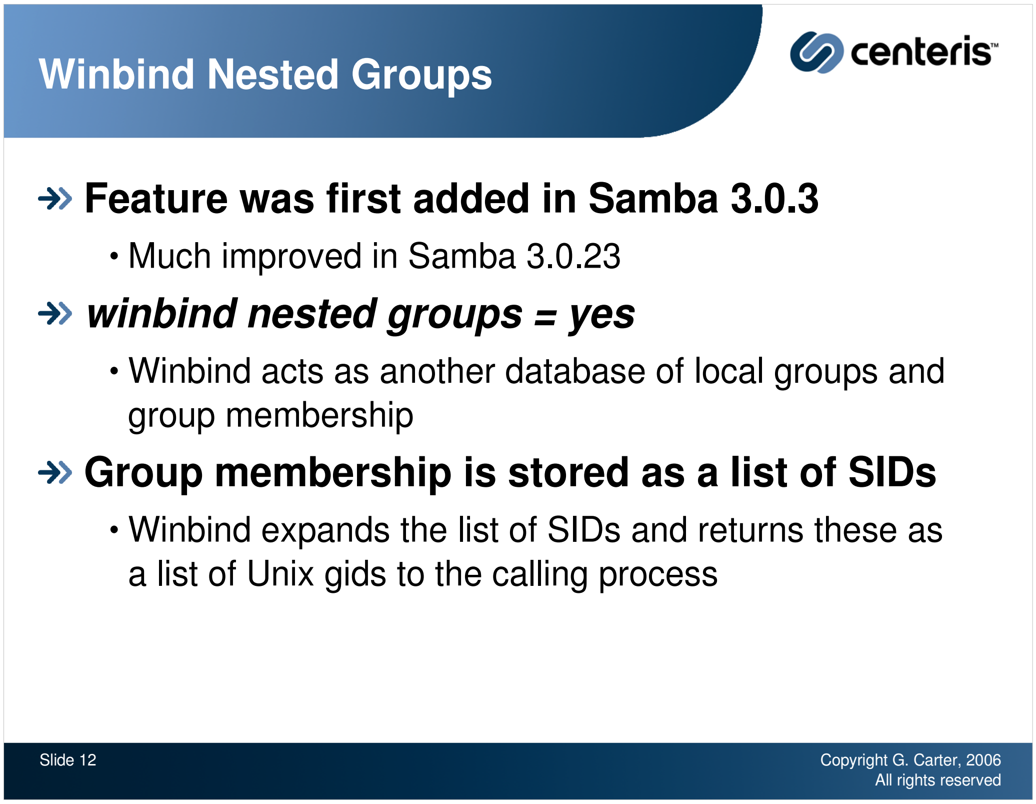
Slide 10



Nesting Groups

- **The Windows NT 4.0 local group model allows a server to define a group that may contain**
  - Local and Domain users
  - Domain Groups
- **Example:**
  - Adding the Domain Admins group to the local Administrators group

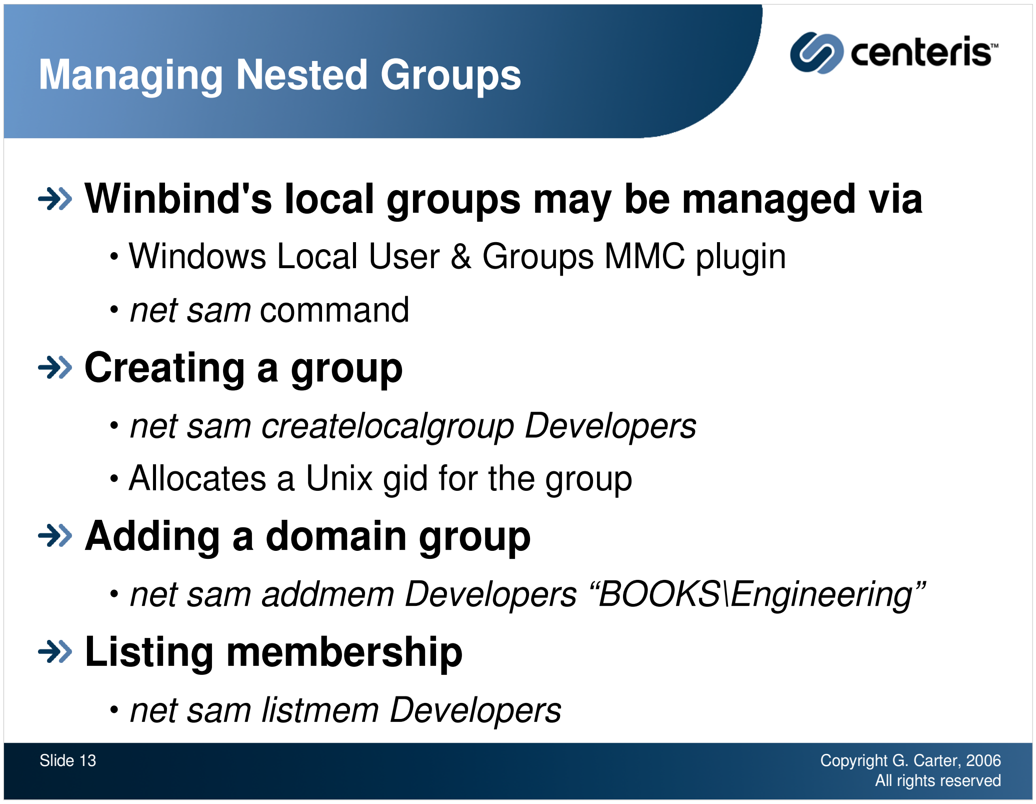
Slide 11



Winbind Nested Groups

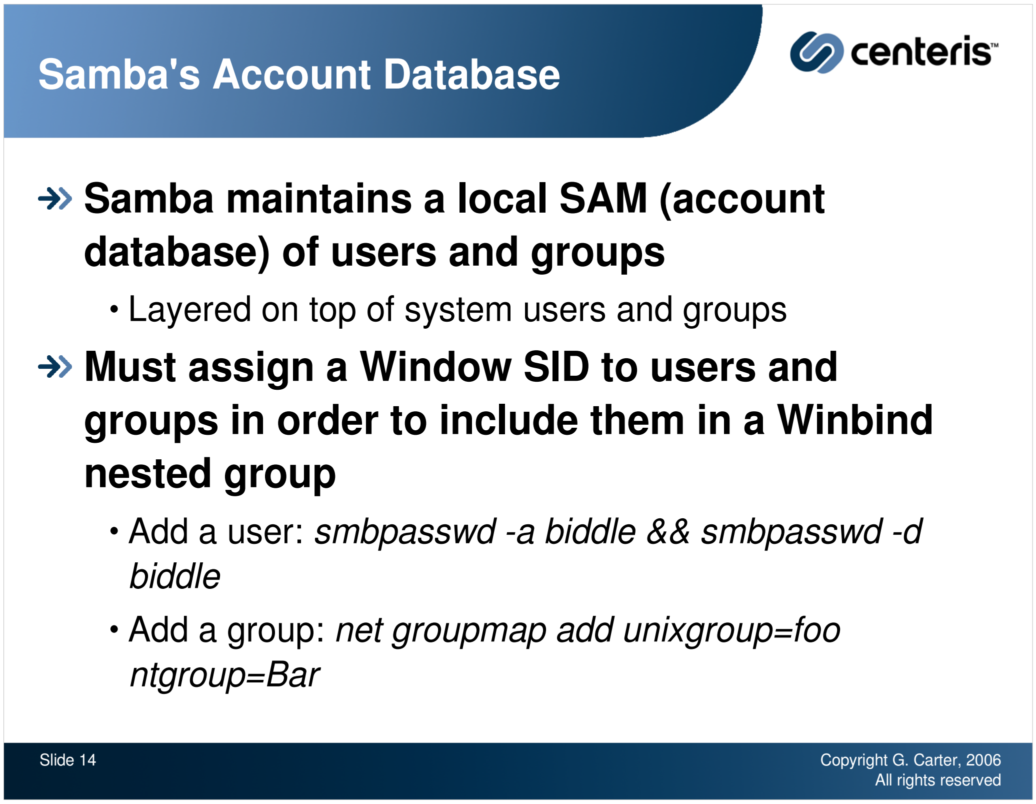
- **Feature was first added in Samba 3.0.3**
  - Much improved in Samba 3.0.23
- ***winbind nested groups = yes***
  - Winbind acts as another database of local groups and group membership
- **Group membership is stored as a list of SIDs**
  - Winbind expands the list of SIDs and returns these as a list of Unix gids to the calling process

Slide 12



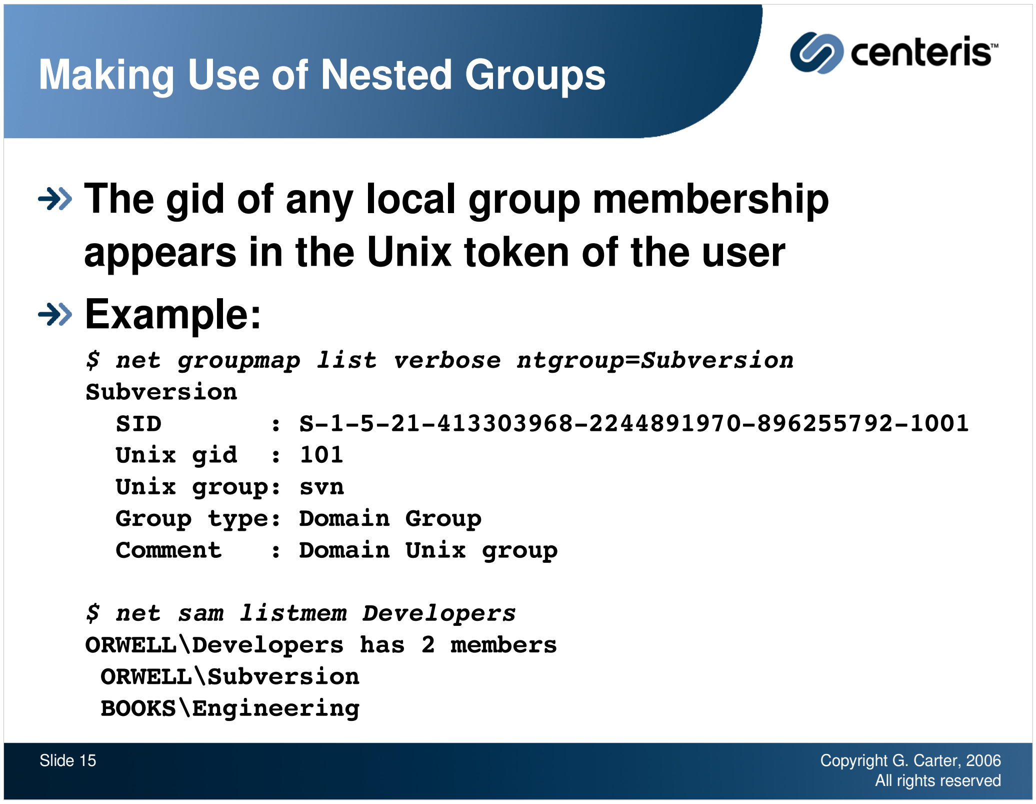
Managing Nested Groups

- **Winbind's local groups may be managed via**
  - Windows Local User & Groups MMC plugin
  - *net sam* command
- **Creating a group**
  - *net sam createlocalgroup Developers*
  - Allocates a Unix gid for the group
- **Adding a domain group**
  - *net sam addmem Developers “BOOKS\Engineering”*
- **Listing membership**
  - *net sam listmem Developers*



Samba's Account Database

- **Samba maintains a local SAM (account database) of users and groups**
  - Layered on top of system users and groups
- **Must assign a Window SID to users and groups in order to include them in a Winbind nested group**
  - Add a user: *smbpasswd -a biddle && smbpasswd -d biddle*
  - Add a group: *net groupmap add unixgroup=foo ntgroup=Bar*

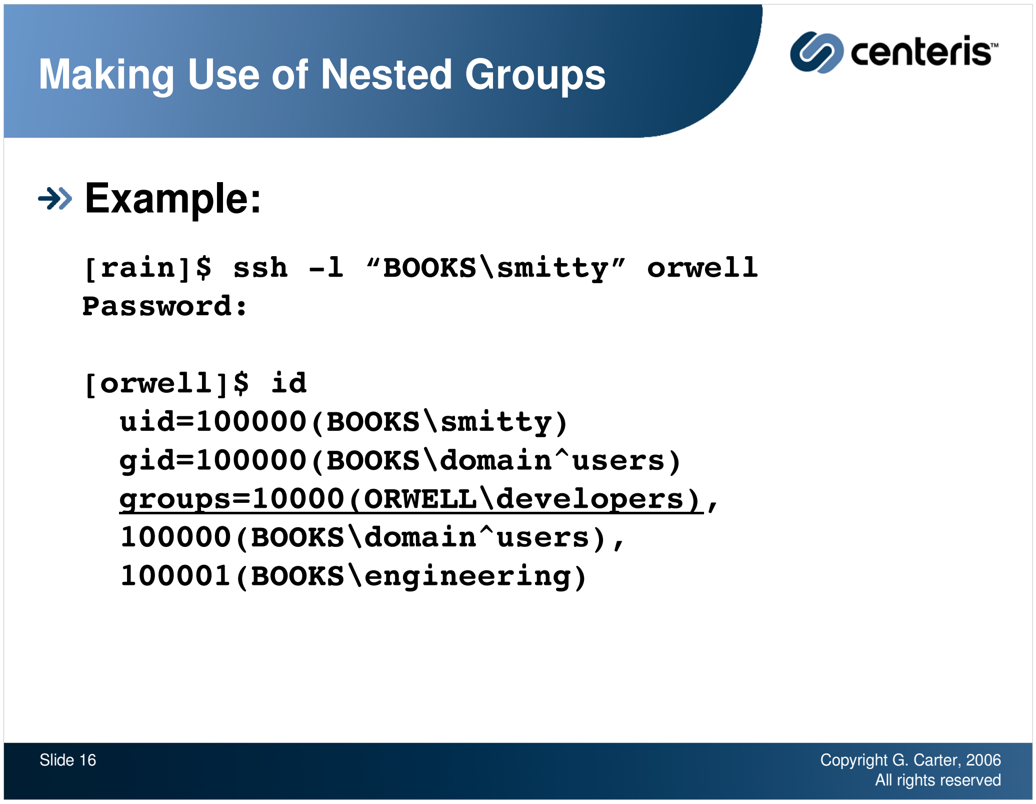


Making Use of Nested Groups

- The gid of any local group membership appears in the Unix token of the user
- Example:

```
$ net groupmap list verbose ntgroup=Subversion
Subversion
  SID        : S-1-5-21-413303968-2244891970-896255792-1001
  Unix gid   : 101
  Unix group: svn
  Group type: Domain Group
  Comment    : Domain Unix group

$ net sam listmem Developers
ORWELL\Developers has 2 members
 ORWELL\Subversion
 BOOKS\Engineering
```

Slide 15

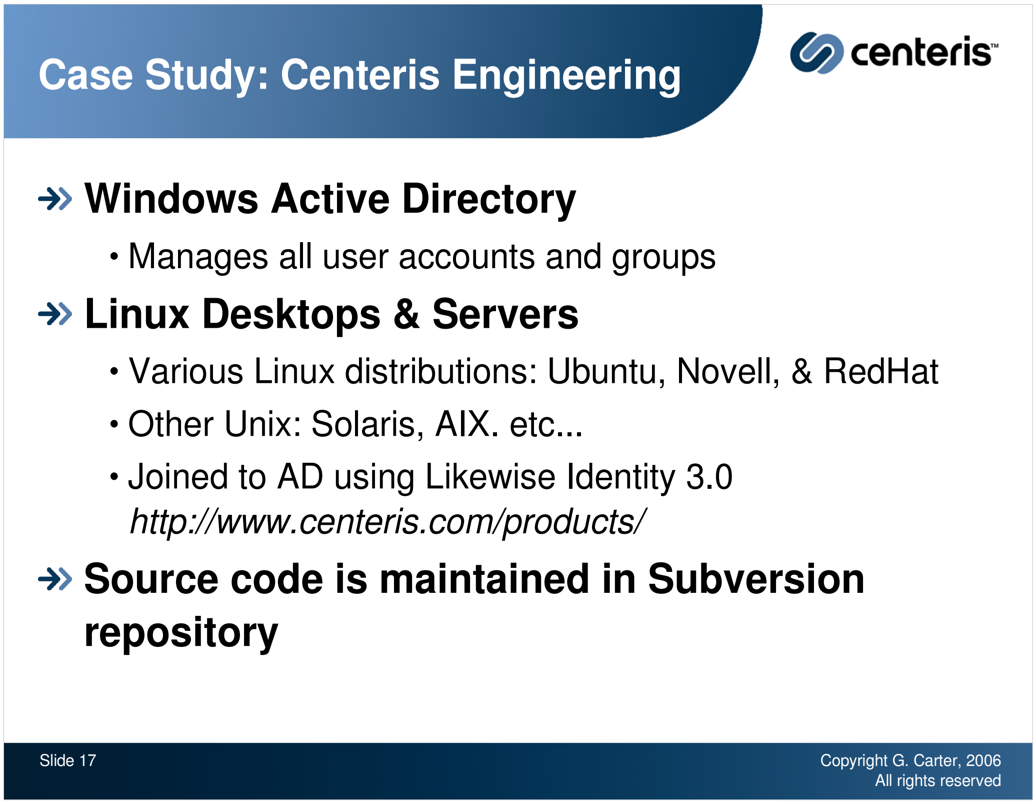


Making Use of Nested Groups

- Example:

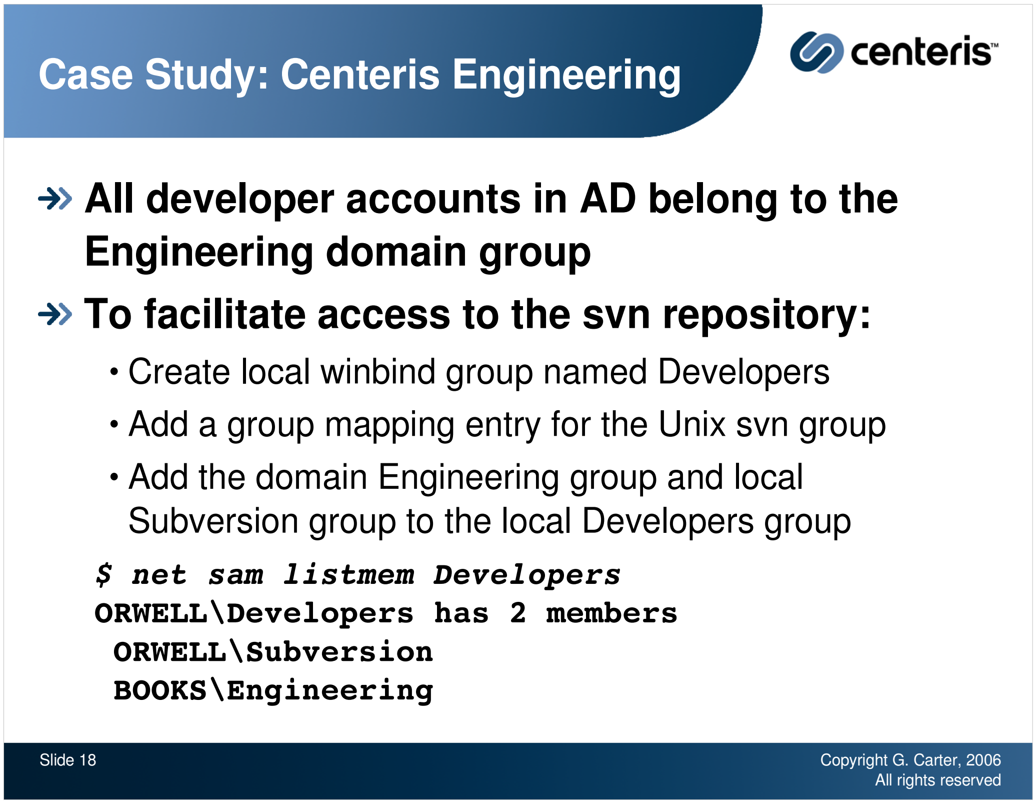
```
[rain]$ ssh -l “BOOKS\smitty” orwell
Password:

[orwell]$ id
  uid=100000(BOOKS\smitty)
  gid=100000(BOOKS\domain^users)
  groups=10000(ORWELL\developers),
  100000(BOOKS\domain^users),
  100001(BOOKS\engineering)
```

Slide 16



Case Study: Centeris Engineering

- **Windows Active Directory**
  - Manages all user accounts and groups
- **Linux Desktops & Servers**
  - Various Linux distributions: Ubuntu, Novell, & RedHat
  - Other Unix: Solaris, AIX. etc...
  - Joined to AD using Likewise Identity 3.0 *http://www.centeris.com/products/*
- **Source code is maintained in Subversion repository**



Case Study: Centeris Engineering

- **All developer accounts in AD belong to the Engineering domain group**
- **To facilitate access to the svn repository:**
  - Create local winbind group named Developers
  - Add a group mapping entry for the Unix svn group
  - Add the domain Engineering group and local Subversion group to the local Developers group

```
$ net sam listmem Developers
ORWELL\Developers has 2 members
 ORWELL\Subversion
 BOOKS\Engineering
```

Case Study: Centeris Engineering

centeris™

- **Group write access is given to the local Developers group**

```
$ ls -ld /data/svn/centeris
drwxrws--- 7 svn ORWELL\developers /data/svn/centeris
```

- **Advantages:**
  - New users and groups may be given access to the svn tree by simply adding the account to the local Developers group
  - The Developers group only has to be managed on the server hosting the svn repository

Questions?

centeris™

Unifying Authorization Models

***Merging /etc/group and
'Domain Users'***

Gerald Carter
Centeris
jerry@samba.org
http://www.samba.org/