Active Directory as AFS' KDC

Derrick Brashear

June 14, 2006

Step 1: Active Directory

- Become an admin in your Active Directory domain.
- Manage users.

win2003 – Parallels Desktop

Manage Your Server

Manage Your Server

Server: WIN2003

Search Help and Support Center

Managing Your Server Roles

Use the tools and information found here to add or remove roles and perform your daily administrative tasks.

- Add or remove a role
- Read about server roles
- Read about remote administration

Your server has been configured with the following roles:

Domain Controller (Active Directory)

Domain controllers use Active Directory to manage network resources such as users, computers, and applications.

- Manage users and computers in Active Directory
- Manage domains and trusts
- Manage sites and services

Tools and

Administra
More Tools
Windows U
Computer Informatio
Internet E
Security C

See Also

Help and S
Microsoft
Deploymer
List of Com
Tasks
Windows S

60 days left for activation

To activate Windows now, click here

Start | Manage Your Server | 8:24 AM

Click inside Guest OS console to capture input

win2003 - Parallels Desktop

Active Directory Users and Computers

File Action View Window Help

Active Directory Users and Computers
- Saved Queries
- ad.dementia.org

Active Directory Users and Computers [win2003.ad.dementia.org] 2 objects

Name	Type	Description
Saved Queries		Folder to store your favor...
ad.dementia....	Domain	

Start | Manage Yo... | Active Direc... | Active Direc... | Active Dir... | 8:25 AM

Click inside Guest OS console to capture input

win2003 - Parallels Desktop

Active Directory Users and Computers

File Action View Window Help

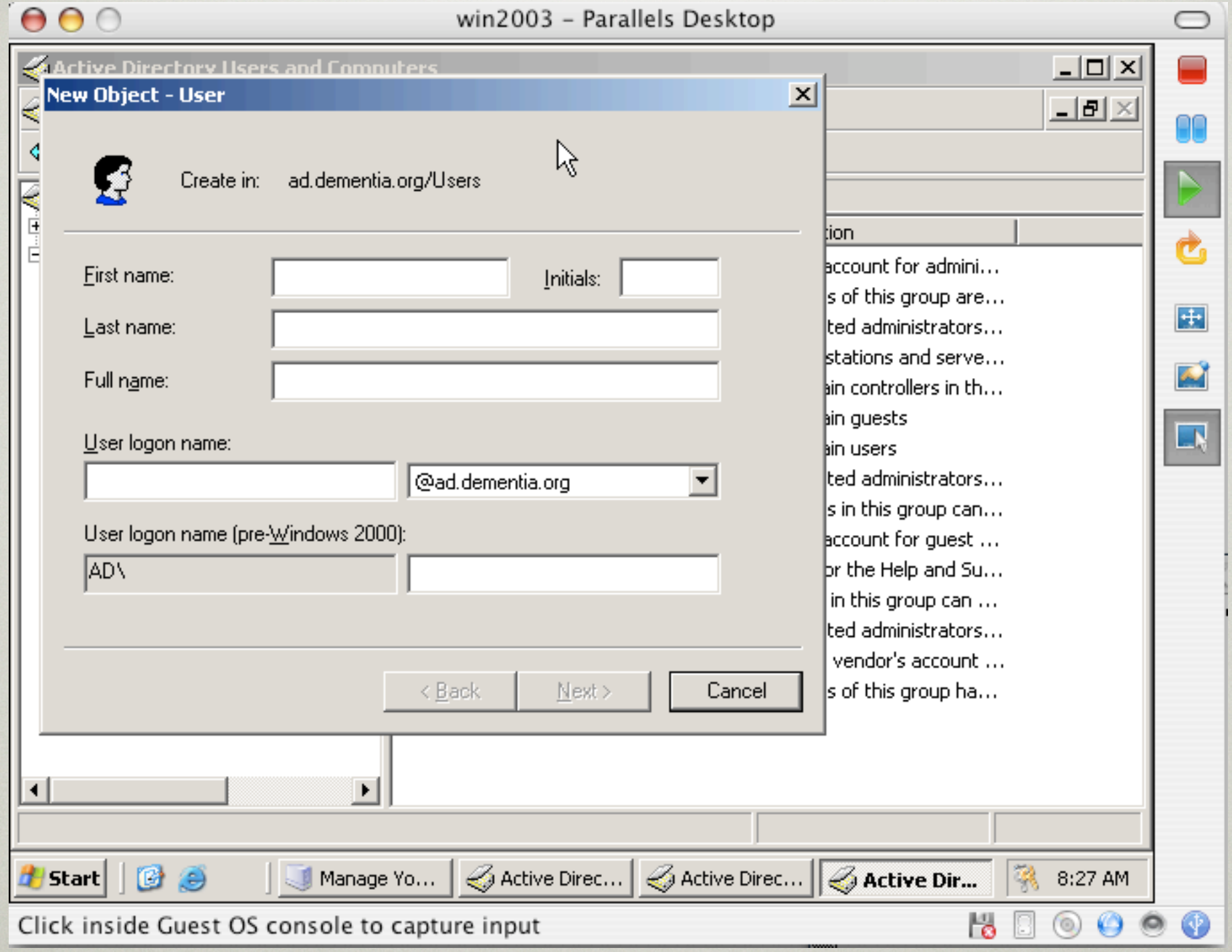
Active Directory Users and Computers
- Saved Queries
- ad.dementia.org
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Users

Users 15 objects

Name	Type	Description
Administrator	User	Built-in account for admini...
Cert Publishers	Security Group ...	Members of this group are...
Domain Admins	Security Group ...	Designated administrators...
Domain Comp...	Security Group ...	All workstations and serve...
Domain Contr...	Security Group ...	All domain controllers in th...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Ad...	Security Group ...	Designated administrators...
Group Policy ...	Security Group ...	Members in this group can...
Guest	User	Built-in account for guest ...
HelpServices...	Security Group ...	Group for the Help and Su...
RAS and IAS ...	Security Group ...	Servers in this group can ...
Schema Admins	Security Group ...	Designated administrators...
SUPPORT_38...	User	This is a vendor's account ...
TelnetClients	Security Group ...	Members of this group ha...

Start | Manage Yo... | Active Direc... | Active Direc... | Active Dir... | 8:26 AM

Press Ctrl+Alt to release keyboard and mouse


win2003 - Parallels Desktop
Active Directory Users and Computers
New Object - User
Create in: ad.dementia.org/Users
First name:
Initials:
Last name:
Full name:
User logon name:
@ad.dementia.org
User logon name (pre-Windows 2000):
AD\
< Back
Next >
Cancel
Start
Manage Yo...
Active Direc...
Active Direc...
Active Dir...
8:27 AM
Click inside Guest OS console to capture input

Make users

- Here, I created myself.

win2003 - Parallels Desktop

Active Directory Users and Computers

New Object - User

Create in: ad.dementia.org/Users

First name: Derrick

Initials: J

Last name: Brashear

Full name: Derrick J. Brashear

User logon name:

shadow

@ad.dementia.org

User logon name (pre-Windows 2000):

AD\

shadow

< Back

Next >

Cancel

account for admini...
s of this group are...
ted administrators...
stations and serve...
ain controllers in th...
ain guests
ain users
ted administrators...
s in this group can...
account for guest ...
or the Help and Su...
in this group can ...
ted administrators...
vendor's account ...
s of this group ha...

Start | Manage Yo... | Active Direc... | Active Direc... | Active Dir... | 8:28 AM

Click inside Guest OS console to capture input

win2003 - Parallels Desktop

Active Directory Users and Computers

File Action View Window Help

Active Directory Users and Computers
- Saved Queries
- ad.dementia.org
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Users

Users 16 objects

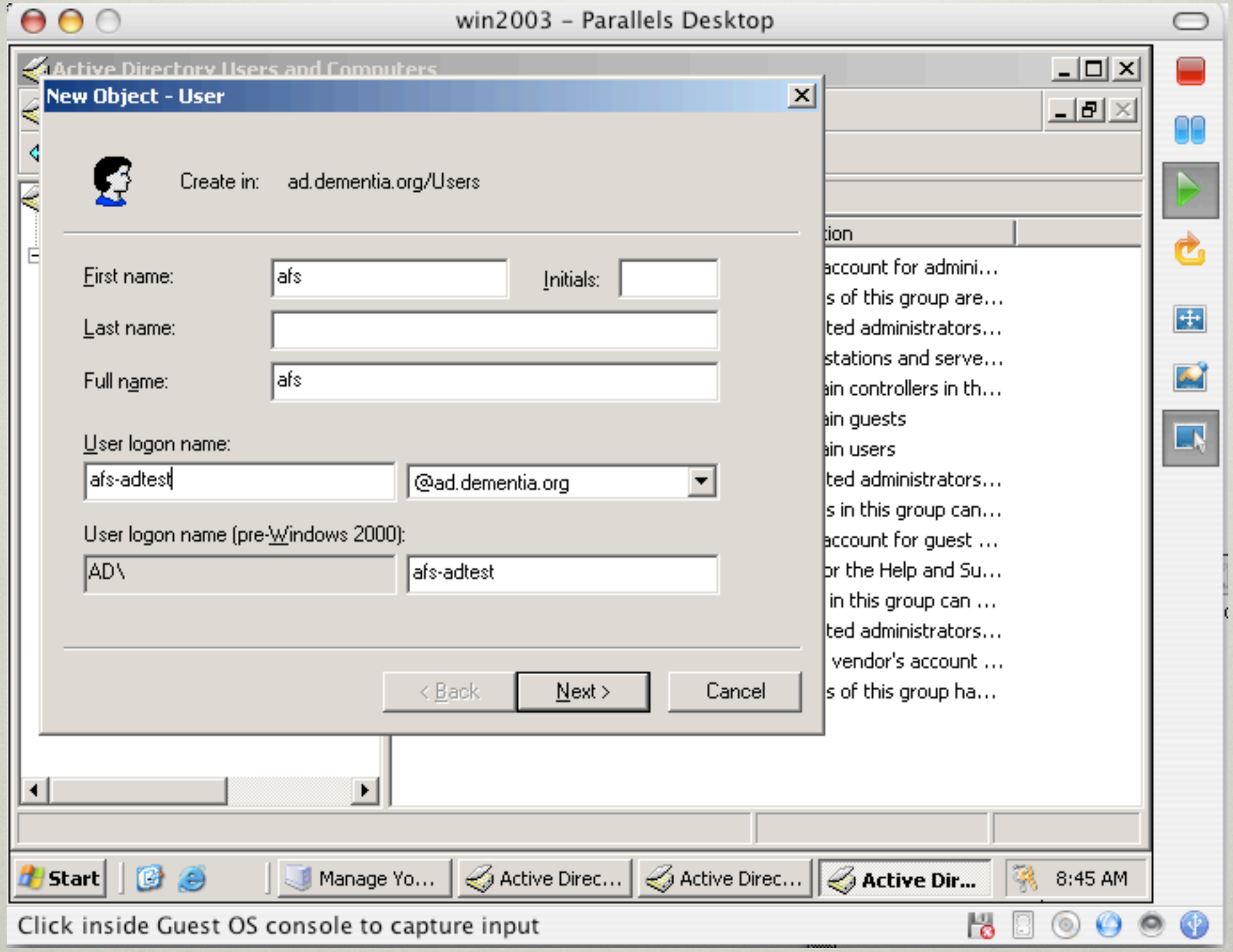
Name	Type	Description
Administrator	User	Built-in account for admini...
Cert Publishers	Security Group ...	Members of this group are...
Derrick J. Bra...	User	
Domain Admins	Security Group ...	Designated administrators...
Domain Comp...	Security Group ...	All workstations and serve...
Domain Contr...	Security Group ...	All domain controllers in th...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Ad...	Security Group ...	Designated administrators...
Group Policy ...	Security Group ...	Members in this group can...
Guest	User	Built-in account for guest ...
HelpServices...	Security Group ...	Group for the Help and Su...
RAS and IAS ...	Security Group ...	Servers in this group can ...
Schema Admins	Security Group ...	Designated administrators...
SUPPORT_38...	User	This is a vendor's account ...
TelnetClients	Security Group ...	Members of this group ha...

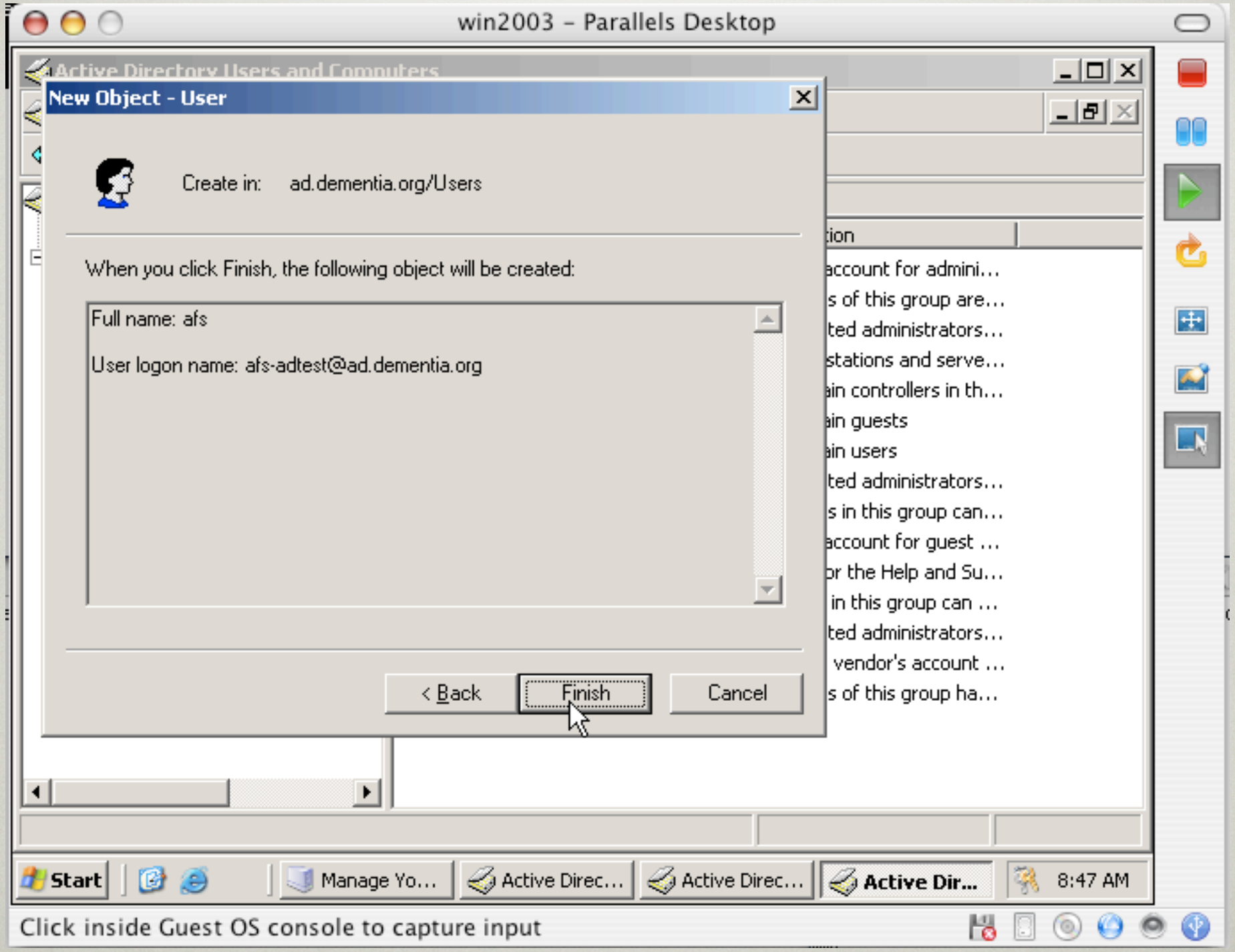
Start | Manage Yo... | Active Direc... | Active Direc... | Active Dir... | 8:29 AM

Click inside Guest OS console to capture input

And services

- Now, create AFS.
- You will be remapping to a principal later, so don’t worry about the name you use here.


win2003 - Parallels Desktop
Active Directory Users and Computers
New Object - User
Create in: ad.dementia.org/Users
First name: afs
Initials:
Last name:
Full name: afs
User logon name:
afs-adtest
@ad.dementia.org
User logon name (pre-Windows 2000):
AD\
afs-adtest
< Back
Next >
Cancel
account for admini...
s of this group are...
ted administrators...
stations and serve...
ain controllers in th...
ain guests
ain users
ted administrators...
s in this group can...
account for guest ...
or the Help and Su...
in this group can ...
ted administrators...
vendor's account ...
s of this group ha...
Start
Manage Yo...
Active Direc...
Active Direc...
Active Dir...
8:45 AM
Click inside Guest OS console to capture input


win2003 - Parallels Desktop
Active Directory Users and Computers
New Object - User
Create in: ad.dementia.org/Users
When you click Finish, the following object will be created:
Full name: afs
User logon name: afs-adtest@ad.dementia.org
< Back
Finish
Cancel
Start
Manage Yo...
Active Direc...
Active Direc...
Active Dir...
8:47 AM
Click inside Guest OS console to capture input

Bind and Export

- Bind a Kerberos principal name
- Export a keytab
- ktpass is in the Support Tools directory on your Windows 2003 media.

win2003 - Parallels Desktop

ktpass.exe

Command Prompt

```
C:\Documents and Settings\Administrator\Desktop>
C:\Documents and Settings\Administrator\Desktop>
C:\Documents and Settings\Administrator\Desktop>
C:\Documents and Settings\Administrator\Desktop>
C:\Documents and Settings\Administrator\Desktop>
C:\Documents and Settings\Administrator\Desktop>
C:\Documents and Settings\Administrator\Desktop>
C:\Documents and Settings\Administrator\Desktop>
C:\Documents and Settings\Administrator\Desktop>
C:\Documents and Settings\Administrator\Desktop>
C:\Documents and Settings\Administrator\Desktop>ktpass -princ afs/adtest.dementi
a.org@AD.DEMENTIA.ORG -mapuser afs -pass * -crypto DES-CBC-MD5 -out afs-keytab
Targeting domain controller: win2003.ad.dementia.org
Using legacy password setting method
Successfully mapped afs/adtest.dementia.org to afs-adtest.
Type the password for afs/adtest.dementia.org:
Type the password again to confirm:
WARNING: pType and account type do not match. This might cause  problems.
Key created.
Output keytab to afs-keytab:
Keytab version: 0x502
keysize 66 afs/adtest.dementia.org@AD.DEMENTIA.ORG ptype 0 (KRB5_NT_UNKNOWN) vno
 3 etype 0x3 (DES-CBC-MD5) keylength 8 (0x374585bc6d5e9783)

C:\Documents and Settings\Administrator\Desktop>_
```

Start | Manage Your Server | 3 Microsoft Mana... | Command Prompt | 8:56 AM

Click inside Guest OS console to capture input

Try It

- Make sure your new realm is in krb5.conf on client(s).
- kinit as a client and see what happens.

xterm

```
                default_domain = xp.win.cmu.edu
        }

        AD.CMU.EDU = {
                kdc = nt-ad2.ad.cmu.edu
                kdc = nt-ad3.ad.cmu.edu
                admin_server = nt-ad2.ad.cmu.edu
                default_domain = ad.cmu.edu
        }

        ANDREW.AD.CMU.EDU = {
                kdc = andrew-ad1.andrew.ad.cmu.edu
                kdc = andrew-ad2.andrew.ad.cmu.edu
                admin_server = andrew-ad2.andrew.ad.cmu.edu
                default_domain = andrew.ad.cmu.edu
        }
        AD.DEMENTIA.ORG = {
                kdc = 10.0.1.60
                default_domain = ad.dementia.org
        }
[v4 realms]
        ATHENA.MIT.EDU = {
                kdc = kerberos.mit.edu
```

xterm

```
Resolving www.dementia.org... 128.2.120.184
Connecting to www.dementia.org|128.2.120.184|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 8,003 (7.8K) [text/plain]

100%[===================================>] 8,003         12.35K/s

10:21:45 (12.34 KB/s) - `edu.mit.Kerberos' saved [8003/8003]

[va1dev08:/Library/Preferences] root# vi edu.mit.Kerberos
[va1dev08:/Library/Preferences] root# exit
exit
[va1dev08:/Library/Preferences] shadow% kinit shadow@AD.DEMENTIA.ORG
Please enter the password for shadow@AD.DEMENTIA.ORG:
[va1dev08:/Library/Preferences] shadow% klist
Kerberos 5 ticket cache: 'API:Initial default ccache'
Default principal: shadow@AD.DEMENTIA.ORG

Valid Starting     Expires            Service Principal
06/14/06 10:23:38  06/14/06 10:48:38  krbtgt/AD.DEMENTIA.ORG@AD.DEMENTIA.ORG
        renew until 06/21/06 10:23:38

klist: No Kerberos 4 tickets in credentials cache
[va1dev08:/Library/Preferences] shadow%
```

Add to Keyfile

- Copy the keytab you got with ktpass to the AFS server.
- Use asetkey to add the key.

xterm

```
[va1dev08:/usr/afs/bin] root# asetkey add 3 ~/afs-keytab afs/adtest.dementia.org
@AD.DEMENTIA.ORG
[va1dev08:/usr/afs/bin] root# bos listkeys localhost
bos: no such entry (getting tickets)
bos: running unauthenticated
key 3 has cksum 2284468697
Keys last changed on Wed Jun 14 10:43:39 2006.
All done.
[va1dev08:/usr/afs/bin] root#
```

Ready to go!

- At this point, tokens you get with aklog are all you need.

xterm

```
[va1dev08:~] shadow% kinit shadow@AD.DEMENTIA.ORG
Please enter the password for shadow@AD.DEMENTIA.ORG:
[va1dev08:~] shadow% aklog adtest.dementia.org -k AD.DEMENTIA.ORG
[va1dev08:~] shadow% tokens

Tokens held by the Cache Manager:

User's (AFS ID 100) tokens for afs@adtest.dementia.org [Expires Jun 14 12:41]
   --End of list--
[va1dev08:~] shadow%
```

Consider disabling PACs

- http://support.microsoft.com/kb/832572/en-us

Active Directory as AFS' KDC

Questions?

shadow@openafs.org