

Windows Manageability News & Analysis

Win2000 TargetSearch™

Search our content and thousands of pre-screened web sites.

POWERED BY
Google

Advanced Search

SITE SPONSOR



Top 10 Active Directory management bloopers

By **Jan Stafford, site editor**
23 Jan 2002, **searchWindowsManageability**

[← More headlines](#)
[→ E-mail a friend](#)

The only consolation for IT managers who make mistakes in Microsoft Active Directory (AD) migration and management is that they're not alone. After helping folks migrate and manage AD over the last couple of years, migration expert Doug Davis has seen more than his share of bloopers. In fact, he's compiled a list of Active Directory blunders that can help you avoid being company to those in AD misery. Davis is product manager, FastLane Migrator, Microsoft Solutions for Irvine, Calif.-based Quest Software

1. *Don't test Replication prior to going live*
This one is repeated time and again. "Replication is the lifeblood of an Active Directory and when it doesn't work properly, late nights ensue," said Davis. If you don't plan, test and prepare for replication, you'll end up in the AD hall of shame.
2. *Install the first Domain Controller without any planning*
The first step to bringing up AD is, of course, to install the root server. Prior to this step you should have planned your forest, determined naming standards, etc. "Many people don't because they are anxious to jump in and start having fun with the system," said Davis. "This often leaves them with awkward forest names or the pain of having to start the entire process over again."
3. *Neglect DNS*
Without DNS there isn't a whole lot you can do with Active Directory. In Active Directory, DNS is King, and has to be treated as such. Many companies neglect planning their DNS infrastructure and immediately get into problems trying to do such things as add new domain controllers to the forest, or connect to the directory -- basically anything that is required to really use Active Directory. DNS in Active Directory isn't just about PING. "You need to understand how your DNS infrastructure works and whether it will be able to support Active Directory's requirement for dynamic DNS and service resource record maintenance," explained Davis.
4. *Manage Active Directory as if it were NT*
This seems to make sense, but a surprising number of IT managers don't take advantage of the new management capabilities of AD, treating it in much the same fashion as NT. "AD is not NT," Davis asserted. "Don't add everyone to the Enterprise Admin group. Continue to ask yourself, 'Why am I not using native delegation?'" The delegation engine in Active Directory is extensive and robust. "Ignore it, and things will get ugly," he warned.
5. *Have a complicated Naming Standard*
Numbers can be easily sorted, but they make lousy naming conventions because who can remember if Rebecca is IK000098 or IK90887? Davis spent many minutes watching network administrators hunt and peck for the account they need. Then they end up calling the end user to say, "What is your network ID again?" It doesn't matter whether you use attributes in AD or you add one yourself, "just don't clutter up the full name or display name with info that can't be used," Davis said.
6. *Deploy too many forests, domains, OUs*
"We see this all the time," Davis said. "It's fun to create new forests, domains or OUs, but the price is administratively so high that we wonder why our customers get trigger happy to add new entities." Always ask yourself, honestly, why one forest, one domain and one OU isn't enough. Question every addition. "We have had to go into companies and do bulk re-orders of OU structures when folks just got out of hand," said Davis. "When you start deploying GPOs into a five domain, 300 OU AD deployment, things get messy fast." When

you consider the amount of administrative delegation you can do with native delegation, those extra OUs often don't help out as much as you might think.

7. *Deploy GPOs without understanding what they do*
Group Policy Objects are powerful tools to ensure that the end user experience is exactly what is required, that security policies are enforced, and that crucial software is published and deployed. "Just jump right in, however, and you will make systems unusable," Davis said. "Read up on GPOs, understand what they can do, and deploy them gradually. You will thank me for this one!"
8. *Go nuts with Schema Extensions*
Active Directory now has a robust schema that can be easily added to, but you have to be careful. Adding new attributes that are not static (i.e. you can make many changes to them) will bog replication down. Also, attributes can only be disabled immediately after they have been added, so you will be stuck with attributes you don't want if you're not careful. "It's not scary stuff; just plan for it," Davis advised.
9. *Add too many attributes to your Global Catalog*
The Global Catalog is a quick search engine for AD and is used extensively by your end-users. "Quite a few times, we have been called in to improve the speed of queries," Davis noted. Why? Admins have added attributes to the Global Catalog in order to help with specific queries, which unfortunately, completely bogged down the Catalog. Keep it simple.
10. *Use ADSIEdit with abandon*
"ADSIEdit (available from the resource kit) is a cool tool because it allows you to get right into the attribute settings for any object," said Davis. In this way, it is similar to the raw property mode of Exchange Administrator. "However, just because you can see an attribute value doesn't mean you should change it," he warned. "And sometimes when you change values, you can't change them back." Determine what the attribute in question does and why you think it should be modified before mucking around it there.

Finally, a good way to avoid mistakes is to use MSDN. This is a treasure trove of faithfully updated information, said Davis. Yet, many IT professionals are unaware of this resource. "Go to www.msdn.microsoft.com and check on your issue before you do anything else," he advised. You could find information there that will help you avoid landing on Davis' blooper list!

For more information:

[Ten Active Directory migration tips](#)

[Tips for planning an Active Directory deployment](#)

EXPLORE THIS AREA: RICH-MEDIA ADVERTISEMENT

@BUSINESS INFRASTRUCTURE

HACKERS ARE KNOCKING.

Click to set the locks << and protect your vital systems.

<< Click for a free anti-hacker book.

IBM

LATEST NEWS

- >> [Gartner predicts major consulting acquisitions in Microsoft's future](#) (ENT Magazine)
- >> [Windows XP Service Pack in view](#) (IDG News)
- >> [Web-based CRM vendors discount Microsoft's move](#) (IDG News)
- >> [Oops! Britney e-mail worm wiggling thru cyberspace](#) (Reuters)
- >> [HTTP must go says Microsoft designer](#) (vnunet)

What's New

1. [Meet Our New Expert, Dr. Thomas Shinder](#)
2. [LISTEN UP. To Win2000Talk Radio](#)
3. [Live Event! Effective Load Balancing](#)
4. [Know IT All Question of the Day](#)

**Limited
Security Budget?**



[Home](#) | [Search](#) | [News](#) | [Best Web Links](#) | [Books, Training & Research](#)

[About Us](#) | [Contact Us](#) | [For Advertisers](#) | [For Business Partners](#) | [Career Center Contacts](#)



[TechTarget Home Page](#) | [Media Kit](#)

The Leading Network of Enterprise IT Web Sites

APPLICATIONS:

[SearchCRM.com](#)
[SearchEBusiness.com](#)
[SearchSAP.com](#)
[SearchWebManagement.com](#)

CORE TECHNOLOGIES:

[SearchDatabase.com](#)
[SearchSecurity.com](#)
[SearchStorage.com](#)
[SearchSystemsManagement.com](#)
[SearchWebServices.com](#)
[Whatis.com](#)

NETWORKING:

[SearchNetworking.com](#)

DEVELOPMENT:

[SearchVB.com](#)

PLATFORMS:

[Search390.com](#)
[Search400.com](#)
[SearchDomino.com](#)
[SearchHP.com](#)
[SearchSolaris.com](#)
[SearchWin2000.com](#)
[SearchWindowsManageability.com](#)

[TechTarget Enterprise IT Conferences](#)

All Rights Reserved, Copyright 2001 - 2002, TechTarget

[Read our Privacy Statement](#)