

Top Ten Troublesome Tweets about Active Directory

*Written by
Don Jones
Co-founder, Concentrated Technology and Microsoft MVP*



White Paper

© Copyright Quest® Software, Inc. 2009. All rights reserved.

This guide contains proprietary information, which is protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software, Inc.

WARRANTY

The information contained in this document is subject to change without notice. Quest Software makes no warranty of any kind with respect to this information. QUEST SOFTWARE SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTY OF THE MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Quest Software shall not be liable for any direct, indirect, incidental, consequential, or other damage alleged in connection with the furnishing or use of this information.

TRADEMARKS

All trademarks and registered trademarks used in this guide are property of their respective owners.

World Headquarters
5 Polaris Way
Aliso Viejo, CA 92656
www.quest.com
e-mail: info@quest.com
U.S. and Canada: 949.754.8000

Please refer to our Web site for regional and international office information.

April, 2009

CONTENTS

Note: This document is based on a compilation of actual "tweets" that were received by Quest Software via Twitter. To maintain authenticity, the author has chosen to retain the original "tweet" content.

INTRODUCTION	4
10: "AUDITOR JUST LEFT. WE FAILED. ACTIVE DIRECTORY IS NOT UP TO SNUFF."	5
9: "SOMEONE DISABLED ALL USERS IN AN OU [ORGANIZATIONAL UNIT], AND CREATED A BUNCH MORE THAT DON'T HAVE THE RIGHT INFO FILLED OUT. ARGGH!"	6
8: "IS IT POSSIBLE TO AUTHENTICATE MANTIS OFF ACTIVE DIRECTORY? THE DOCUMENTATION SAYS "TODO"!"	7
7: "ACTIVE DIRECTORY RECYCLE BIN: IF YOU DON'T KNOW ABOUT THIS FEATURE IN WINDOWS 2008 R2, THEN THIS MAY SAVE YOUR [JOB]."	8
6: "LOCKING DOWN THE MACS ON CAMPUS WITH ACTIVE DIRECTORY."	9
5: "LOOKING AT AN ACTIVE DIRECTORY WHERE OVER 40% OF THE COMPUTER ACCOUNTS ARE NOT IN USE--ALL IN THE SAME OU. OH SWEET JOY."	10
4: "MICROSOFT ACTIVE DIRECTORY PERMISSIONS ARE A LITTLE MORE COMPLICATED THAN I THOUGHT"	11
3: "USING POWERSHELL TO IMPORT GROUPS INTO A NEW ACTIVE DIRECTORY WITH AD CMDLETS...."	12
2: "I NOW KNOW WHY I LET MY ACTIVE DIRECTORY PASSWORD LAPSE: I COULDN'T FIND MY PASSWORD GENERATOR!"	13
1: "F#&%%#@# ACTIVE DIRECTORY HAS RUINED MY FRIDAY AFTERNOON."	14
APPENDIX: FOLLOW QUEST ON TWITTER	15
ABOUT THE AUTHOR.....	16
ABOUT QUEST SOFTWARE, INC.....	17
CONTACTING QUEST SOFTWARE	17
CONTACTING QUEST SUPPORT	17

INTRODUCTION

Twitter, in case you're not familiar with it, is a "micro-blogging" social networking site where users post their immediate thoughts and activities—in 140 characters or less. You can "follow" specific users' Twitter streams, either online or via RSS, and there are various tools available to help you search Twitter for specific keywords and other tasks.

On any given day, you'll find Twitter.com awash with "tweets" from people who are struggling with Active Directory (AD) management. The truth is that AD is a complex, powerful technology that can be very complicated to manage, especially in today's heterogeneous environments. This paper lists the top ten "tweets" that I found one day, and my thoughts on how to resolve the challenges.

10: "AUDITOR JUST LEFT. WE FAILED. ACTIVE DIRECTORY IS NOT UP TO SNUFF."

There are two kinds of problems that irritate AD auditors: the first is the condition of the AD objects themselves, such as unused user accounts or improper permissions, and the second is the configuration of AD, including certain top-level permissions.

In either case, you can choose one of three ways to fix the problem:

1. Manually review and fix everything.
2. Get reporting tools to find the problems, and then fix them manually.
3. Get tools that are configured to look for and automatically implement the correct configuration.

I prefer option three, but these tools aren't built into Windows—you have to get them via a third-party solution. Good tools can implement proper configuration settings based on selected industry requirements or best practices, including specific compliance efforts. This means that your auditors will love you. The *best* tools can continually scan and enforce those settings automatically—providing you with a compliance "dashboard" and automated remediation. And this means that the next visit by the auditors won't ruin your day.

By the way, don't feel badly that your auditors found a lot to complain about. AD is notoriously difficult to properly configure for specific compliance efforts, simply because it's such a large, complex, distributed system and most compliance efforts contain very little in the way of specific technical guidance. I've found that education—understanding how the compliance requirements map to actual technical specifications—is invaluable. TheExpertsCommunity.com is a great online community for asking those types of questions and getting accurate answers.

9: “SOMEONE DISABLED ALL USERS IN AN OU [ORGANIZATIONAL UNIT], AND CREATED A BUNCH MORE THAT DON’T HAVE THE RIGHT INFO FILLED OUT. ARGGH!”

Disabling all the users—that’s malicious. It could have been mistake, but probably not. And creating a bunch of users and not filling in all of the right attributes? Well, that’s probably just laziness. In either case, this tweet relates to a major challenge in AD: maintaining consistent data and protecting the directory from mistakes.

A good way to address this challenge is to use a change control tool that implements workflow. For example, with this tool in place, the action of disabling a user would need to be reviewed and approved by a peer or senior colleague. Similarly, you can specify certain mandatory attributes to be specified when a user is created and pre-populate some of them based on business rules.

Third-party tools can help control change and implement approval-based workflow, and a good one to start with is Quest’s Active Directory Management Console, better known as ADMC (<http://www.quest.com/free-tools/>). Compatible with any recent version of AD, ADMC lets you specify business and workflow rules. It can even bundle approved changes together in batches to be implemented during maintenance windows.

8: "IS IT POSSIBLE TO AUTHENTICATE MANTIS OFF ACTIVE DIRECTORY? THE DOCUMENTATION SAYS "TODO"!"

Mantis is a PHP-based bug-tracking application. But this tweet is important because you could replace "mantis" with anything, for example, *Is it possible to authenticate (insert application name here) off Active Directory*. Finding documentation that says "TODO" is pretty much par for the course. The trick to solving this problem is being aware that you don't need every single individual application to support AD authentication; rather, you need a central authentication broker that can make a wide variety of applications AD-integrated.

One solution is third-party tools. And some first-party tools, for example, Microsoft's Identity Lifecycle Manager (ILM), integrates certain non-Microsoft applications with AD. In the case of Mantis and many other third-party applications, you'll want to look for an authentication-integration tool that can work generically with database-driven applications. Surprisingly, such tools do exist, and some work in conjunction with strong-authentication tools like smart cards or authentication keys.

Of course, you could just wait for every application vendor to incorporate AD authentication. Honestly, though, a lot of them haven't even progressed enough to put "TODO" in their documentation.

7: "ACTIVE DIRECTORY RECYCLE BIN: IF YOU DON'T KNOW ABOUT THIS FEATURE IN WINDOWS 2008 R2, THEN THIS MAY SAVE YOUR [JOB]."

No kidding! It's tough to believe that the company that invented the desktop "Recycle Bin" took eight years to add it to something as critical as AD. It's a great feature, even though there is no user interface. Of course, third parties have provided Recycle Bin-style single-object recovery since AD first launched in Windows 2000, and many of those third-party tools continue to thrive because they offer a richer feature set than the built-in Recycle Bin.

AD recovery is tricky. For example, if you recover a group, do you also need to recover any members it may have contained? What about recovering an OU: do you also recover its child objects? How would you do it? The bottom line is that you shouldn't have to keep all those answers in your head: The recovery rules are too complex. Instead, when the built-in Recycle Bin isn't enough, rely on a good third-party tool. The tool *knows* the rules, and can perform them quickly and consistently—and usually without taking a domain controller offline (frankly, that's a must-have feature in my book). One option is to grab "Object Restore for Active Directory" from <http://www.quest.com/object-restore-for-active-directory/>. It acts as a free Recycle Bin for Windows 2000, 2003, or 2008 and will restore the basic attributes of an object without requiring you to restart a domain controller in Directory Service Restore Mode.

6: "LOCKING DOWN THE MACS ON CAMPUS WITH ACTIVE DIRECTORY."

Ah, academia—it is the land of heterogeneous client operating systems. Actually, more and more corporations are also adopting a wider variety of client operating systems. This enables them to adopt the best tools for a variety of jobs. The one thing that you always miss with Windows is the tight integration between the desktop OS and Active Directory, including integrated security and configuration through Group Policy. You can't get that with a Mac or Linux computer!

Or perhaps you can. Group Policy itself is extensible. All you'd need is a client-side piece of software that knows how to (a) authenticate to AD using the industry-standard Kerberos protocol, (b) look for appropriate Group Policy objects (GPOs), and (c) download and implement the GPO settings. Third-party software vendors offer many tools that provide AD-integrated authentication, file sharing, and other basic network services, as well as centralized configuration and control via Group Policy. You can bring your entire Mac and Unix/Linux configurations from both desktops and servers into a single, consistent place and manage them with one set of tools. It's a great way to improve compliance, if you're in a business that is subject to regulatory or industry requirements.

Knowing that these types of tools are available brings you halfway to solving your IT problems; I learned about these at The Experts Conference (<http://theexpertsconference.com>), an annual technical education conference attended by some of the most hardcore AD experts in the world.

5: "LOOKING AT AN ACTIVE DIRECTORY WHERE OVER 40% OF THE COMPUTER ACCOUNTS ARE NOT IN USE--ALL IN THE SAME OU. OH SWEET JOY."

Ouch. That's not only annoying; it'll get you into trouble during an audit. You need to figure out which accounts aren't in use, disable them for a while to make sure, and then finally delete them. Oh, and don't forget to reassign the permissions on any resources owned by those deleted accounts.

Everyone in our industry loves to talk about *provisioning*, but the smart money is on something bigger: *identity lifecycle management*. You have to do more than provision users—you have to re-provision them when their roles in the organization change, and de-provision them when they leave. De-provisioning disables their accounts and re-assigns access permissions. This means that you're not faced with 40% inactive user accounts that are nothing but a security liability.

4: "MICROSOFT ACTIVE DIRECTORY PERMISSIONS ARE A LITTLE MORE COMPLICATED THAN I THOUGHT"

No kidding. The native user interface in AD Users and Computers doesn't make AD permissions any more approachable, either. My advice is to stop dealing with AD permissions entirely. AD permissions are just a piece of the puzzle; you've also got file permissions, printer permissions, Exchange permissions, multiple domains, databases, and file shares. The number of places where you have to manage permissions is mind-boggling. That's why identity and access management (IAM) tools are so powerful; you define *roles* that correspond to the job titles in your organization, assign permissions to those roles, and then tell the tool who is assigned which job title. The tool implements and enforces those permissions on an ongoing basis and creates detailed access reports. You will never have to look at a permissions dialog box again.

3: "USING POWERSHELL TO IMPORT GROUPS INTO A NEW ACTIVE DIRECTORY WITH AD CMDLETS...."

Apparently this tweet is referring to the free AD cmdlets from Quest. These cmdlets gave us a way to automate AD management via Windows PowerShell years before Microsoft was ready to release built-in cmdlets for AD (in Windows Server 2008 R2). Available at www.quest.com/powershell, these cmdlets make it easy to import users, modify users and groups, and more. Imagine starting with a CSV file and running a command like this (where *LoginName*, *FullName*, *Dept*, and *City* are columns in the CSV file):

```
Import-CSV Users.csv | ForEach-Object { New-QADUser -organizationalUnit "ou=users,dc=domain,dc=com" -samAccountName $_.LoginName -Name $_.FullName -Department $_.Dept -City $_.City }
```

You can create a hundred users as quickly as you can create one using the graphical console. And with Windows PowerShell, you can make that command part of a longer command batch (call it a "script" if you want to) that performs other provisioning tasks, like creating home folders and adding the new user to the proper groups.

2: "I NOW KNOW WHY I LET MY ACTIVE DIRECTORY PASSWORD LAPSE: I COULDN'T FIND MY PASSWORD GENERATOR!"

I hate "strong" passwords. They're hard to remember, and they're no more secure than weaker ones. Sure, they might be harder to guess, but if someone has a rainbow table and access to a domain controller (which is perhaps the most fearsome scenario), strong passwords crack as easily as so-called "weak" ones. Rainbow tables capable of cracking ten-character passwords are readily available on a set of DVDs and can crack a "strong" password in under a minute. So how do you keep your password secure?

First, try *passphrases*. Something like "My son's name is Bobby" is easy to remember and would require an *enormous* rainbow table to crack. Second, implement true single sign-on, so that your single AD passphrase grants you access to every enterprise resource. Even better, eliminate passwords entirely and rely on two-factor authentication, such as hardware keys that generate single-user passwords. While some companies use those kinds of keys for remote access users, there's little reason not to use them internally as well. With the right third-party software, you can integrate nearly any industry-standard hardware key with AD and the rest of your enterprise's security systems, creating a single sign-on environment that doesn't require expiring passwords, password generator, or a photographic memory to create and maintain passwords.

1: "F#&%%#@# ACTIVE DIRECTORY HAS RUINED MY FRIDAY AFTERNOON."

This tweet is my favorite of the bunch. Here are some of the reasons why AD has spoiled my Friday afternoons in the past:

- Something broke—usually replication. Tracking down the exact bit of replication that isn't working, along with the exact reason, is tedious. Troubleshooting and monitoring tools that are specifically designed for AD analysis can usually spot the problem and offer advice on solving it.
- Someone asked for a report (Why do they wait until Friday afternoons to do that?) on "who has access to what," or (even worse) "who had access to such-and-such three weeks ago?" Windows doesn't make it easy to get current permissions information, and historical information simply isn't available without an access management tool. By using this tool I can produce the report in five minutes.
- Someone deleted something they shouldn't have. In my case, it always seems to be an entire OU, and they don't tell me about the problem until the change has been replicated through the environment (that's when replication always works perfectly). My solution? Either take a DC offline and start the exciting world of Recovery Mode, or use a good AD recovery tool to recover the specific object I need. Then upgrade to the latest version of Windows and check the "protect from accidental deletion" checkbox on the restored object.
- We get a bunch of new hires. (Human Resources only seems to know about these on Friday afternoons, and of course the folks start first thing on Monday.) This means that I need to create user accounts, assign group memberships and permissions, and so on. A good identity and access management solution makes it easier. Some import new users right from an HR system, but even the simplest tools allow me to drop the new identities into the corresponding job title "roles" and be finished more quickly.

These are all situations that could be easily solved with the right tools. Don't blame Microsoft for not making these tools part of Windows; most of these situations are pretty specific to one type of business or to a specific need. Windows is a generic operating system meant to be used by many different types of organizations. Microsoft relies heavily on independent software vendors (ISVs) to create a competitive marketplace for tools that meet specific business requirements.

APPENDIX: FOLLOW QUEST ON TWITTER

Many of Quest Software's AD experts are on Twitter every day, looking to help with answers for questions like the ones here. They are eager to share their own discoveries and challenges. If you'd like to follow them, look for these Twitter users:

- Chris Ashley (product manager): ChrisAshley_PM
- Shawn Barker (product manager): barkershawn
- Joe Baguley (CTO, Europe): JoeBaguley
- Gil Kirkpatrick (Microsoft MVP): gkirkpatrick
- Rod Simmons (Director of Tech Strategy): RodSimmons
- Michael Twedde (Director of Product Management): mwtwedd
- Bob Bobel (Product Manager): rbobel
- Jonathan Sander (IAM/Access Analyst): jonathansander

ABOUT THE AUTHOR

Don Jones is a co-founder of Concentrated Technology (ConcentratedTech.com), a Microsoft Most Valuable Professional Award recipient, and the author of more than thirty books on information technology. His consulting practice specializes in making the connection between technology and business, helping businesses realize more value from their IT investment, and helping IT align more closely to business needs and values.

Don has been an IT journalist for more than eight years, and is currently a Contributing Editor for *Microsoft TechNet Magazine*. He is also a sought-after speaker at industry conferences and symposia, including Connections conferences, Microsoft TechEd, TechMentor Events, and others.

ABOUT QUEST SOFTWARE, INC.

Quest Software, Inc., a leading enterprise systems management vendor, delivers innovative products that help organizations get more performance and productivity from their applications, databases, Windows infrastructure and virtual environments. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 100,000 customers worldwide meet higher expectations for enterprise IT. Quest also provides customers with client management through its ScriptLogic subsidiary and server virtualization management through its Vizioncore subsidiary. Quest Software can be found in offices around the globe and at www.quest.com.

Contacting Quest Software

Phone: 949.754.8000 (United States and Canada)

Email: info@quest.com

Mail: Quest Software, Inc.
World Headquarters
5 Polaris Way
Aliso Viejo, CA 92656
USA

Web site: www.quest.com

Please refer to our Web site for regional and international office information.

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a commercial version and have a valid maintenance contract. Quest Support provides around the clock coverage with SupportLink, our web self-service. Visit SupportLink at <http://support.quest.com>

From SupportLink, you can do the following:

- Quickly find thousands of solutions (Knowledgebase articles/documents).
- Download patches and upgrades.
- Seek help from a Support engineer.
- Log and update your case, and check its status.

View the **Global Support Guide** for a detailed explanation of support programs, online services, contact information, and policy and procedures. The guide is available at: http://support.quest.com/pdfs/Global_Support_Guide.pdf