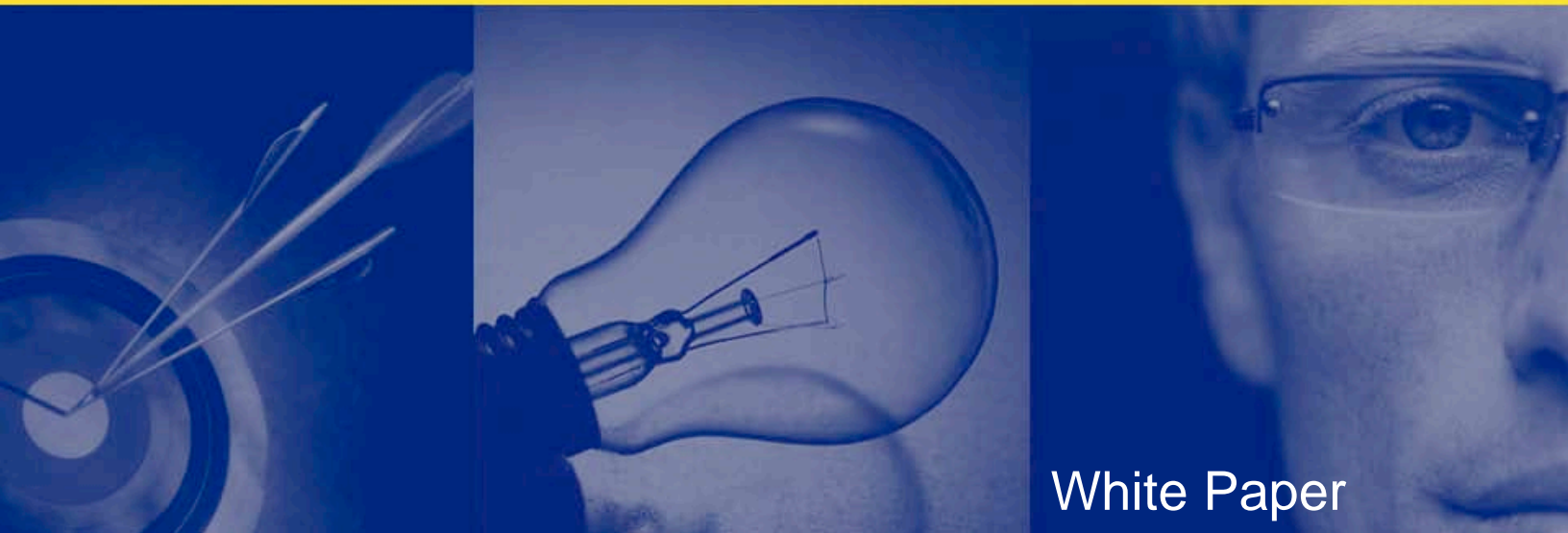


The Active Directory Recycle Bin: The End of Third-Party Recovery Tools?

*Written by
Don Jones
Microsoft MVP*



White Paper

© 2009 Quest Software, Inc. 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

Quest, Quest Software, the Quest Software logo, AccessManager, Aelita, Akonix, AppAssure, Benchmark Factory, Big Brother, BusinessInsight, ChangeAuditor, DataFactory, DeployDirector, DirectoryAnalyzer, DirectoryTroubleshooter, DNS Analyzer, DSExpert, ERDisk, Foglight, GPOAdmin, iToken, I/Watch, Imceda, InLook, IntelliProfile, InTrust, Invirtus, I/Watch, JClass, Jint, JProbe, LeccoTech, LiteSpeed, LiveReorg, LogADmin, MessageStats, Monosphere, NBSpool, NetBase, NetControl, Npulse, NetPro, PassGo, PerformaSure, Quest Central, Quest vToolkit, Quest vWorkSpace, ReportADmin, RestoreADmin, SelfServiceADmin, SharePlex, Sitraka, SmartAlarm, Spotlight, SQL LiteSpeed, SQL Navigator, SQL Watch, SQLab, Stat, StealthCollect, Storage Horizon, Tag and Follow, Toad, T.O.A.D., Toad World, vAutomator, vControl, vConverter, vFoglight, vOptimizer Pro, vPackager, vRanger, vRanger Pro, vSpotlight, vStream, vToad, Vintela, Virtual DBA, VizionCore, Vizioncore vAutomation Suite, Vizioncore vBackup, Vizioncore vEssentials, Vizioncore vMigrator, Vizioncore vReplicator, Vizioncore vTraffic, Vizioncore vWorkflow, Xaffire, and XRT are trademarks and registered trademarks of Quest Software, Inc in the United States of America and other countries. Other 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.

Updated: June, 2009

CONTENTS

INTRODUCTION	4
BACKGROUND: WHEN DELETED DOESN'T MEAN DELETED	5
WELCOME, WINDOWS SERVER 2008 R2 RECYCLE BIN	6
NOT LIKE THE WINDOWS EXPLORER RECYCLE BIN.....	6
UPGRADES REQUIRED.....	6
CAUTION: ONE-WAY ROAD AHEAD.....	7
THIRD-PARTY ACTIVE DIRECTORY RECOVERY TOOLS	8
WHAT ABOUT <i>CHANGES</i> ?.....	8
RECOVERING MULTIPLE OBJECTS OR A HIERARCHY?	9
WHAT ABOUT GROUP POLICY OBJECTS?.....	9
WORRIED ABOUT YOUR FOREST?.....	9
CONCLUSION: THE NEW ACTIVE DIRECTORY RECYCLE BIN VS. THIRD-PARTY RECOVERY TOOLS	10
ABOUT THE AUTHOR	11
ABOUT QUEST SOFTWARE, INC.	12
CONTACTING QUEST SOFTWARE	12
CONTACTING QUEST SUPPORT	12

INTRODUCTION

Windows Server 2008 R2 offers a number of exciting new features, including an expanded Server Core offering, new Active Directory features, and – of special interest to anyone who has ever wished Active Directory had an “undo” button – a sort of recycle bin for Active Directory objects.

Wait – a recycle bin? Does that mean no more rebooting a domain controller into Recovery Mode, and no more need for the many third-party utilities out there that used to provide this type of online, single-object recovery?

Not *exactly*.

BACKGROUND: WHEN DELETED DOESN'T MEAN DELETED

As you may know, deleted objects in Active Directory aren't deleted immediately. Instead, they're marked with a "tombstone" flag, which is replicated to all domain controllers in the domain. Tombstoned objects, as they're called, continue to hang around in the directory for some time – 180 days in the most recent versions of Active Directory. Although they can't be used to log on or for any other purposes, keeping the objects around in this tombstoned condition helps ensure that *every* domain controller knows about the deletion.

Some recycle bin-like tools of the past simply take advantage of the situation, giving you a graphical user interface for seeing tombstoned objects, and enabling you to remove the tombstone flag (and replicate that change), bringing the object back to life – *reanimating* it, to stick with the graveyard terminology. Some third-party recovery tools, especially shareware, provide no other functionality. If you're comfortable using ADSIEdit or other free, low-level tools (or scripts you write yourself) you can change the tombstone attributes yourself.

There's a downside, though: When an object is deleted, Active Directory removes most of its attributes at the same time it applies the tombstone flag. So simply reanimating an object often isn't simple at all. You may also need to repopulate the majority of its attributes to make it fully-functional again.

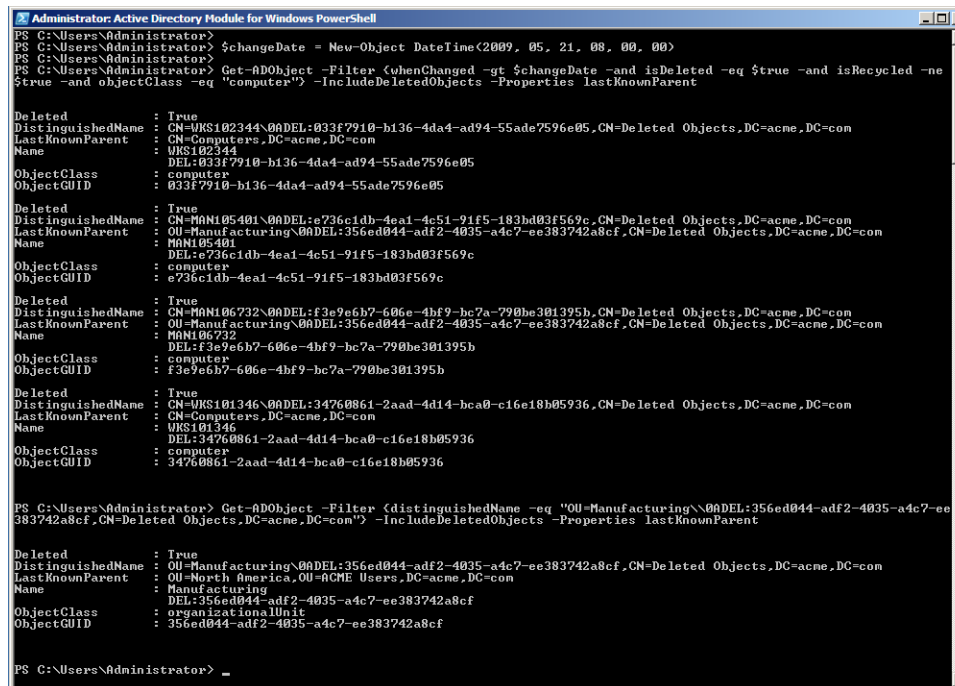
WELCOME, WINDOWS SERVER 2008 R2

RECYCLE BIN

Windows Server 2008 R2 makes one important change to the deleting process: It places deleted objects into a “deleted” state where their attributes are left intact. This means that reanimating a deleted object, by flipping the tombstone flag, is easier, because the object is preserved in its original form. After the Deleted Object lifetime (180 days by default), the object is “recycled,” its attributes are stripped, and the object can no longer be reanimated.

Not Like the Windows Explorer Recycle Bin

Unfortunately, Windows Server 2008 R2 *will not provide an actual recycle bin* in the form of an icon or container that you can use to easily access deleted objects. Deleted objects will still be essentially inaccessible from most native Active Directory management tools, and you’ll need to use low-level directory editors, scripting, or other complex means to reanimate objects from their “deleted” state.



```
Administrator: Active Directory Module for Windows PowerShell
PS C:\Users\Administrator>
PS C:\Users\Administrator> $changeDate = New-Object DateTime(2009, 05, 21, 08, 00, 00)
PS C:\Users\Administrator> Get-ADObject -Filter (whenChanged -gt $changeDate -and isDeleted -eq $true -and isRecycled -ne $true -and objectClass -eq "computer") -IncludeDeletedObjects -Properties lastKnownParent

Deleted : True
DistinguishedName : CN=WKS102344\0ADEL:033F7910-b136-4da4-ad94-55ade7596e05,CN=Deleted Objects,DC=acme,DC=com
LastKnownParent : CN=Computers,DC=acme,DC=com
Name : WKS102344
ObjectClass : computer
ObjectGUID : 033F7910-b136-4da4-ad94-55ade7596e05

Deleted : True
DistinguishedName : CN=MAMI05401\0ADEL:e736c1db-4ea1-4c51-91f5-183bd03f569c,CN=Deleted Objects,DC=acme,DC=com
LastKnownParent : OU=Manufacturing\0ADEL:356ed044-adf2-4035-a4c7-ee383742a8cf,CN=Deleted Objects,DC=acme,DC=com
Name : MAMI05401
ObjectClass : computer
ObjectGUID : e736c1db-4ea1-4c51-91f5-183bd03f569c

Deleted : True
DistinguishedName : CN=MAMI06732\0ADEL:f3e9e6b7-606e-4bf9-hc7a-790be301395b,CN=Deleted Objects,DC=acme,DC=com
LastKnownParent : OU=Manufacturing\0ADEL:356ed044-adf2-4035-a4c7-ee383742a8cf,CN=Deleted Objects,DC=acme,DC=com
Name : MAMI06732
ObjectClass : computer
ObjectGUID : f3e9e6b7-606e-4bf9-hc7a-790be301395b

Deleted : True
DistinguishedName : CN=WKS101346\0ADEL:34760861-2aad-4d14-bca0-c16e18b05936,CN=Deleted Objects,DC=acme,DC=com
LastKnownParent : CN=Computers,DC=acme,DC=com
Name : WKS101346
ObjectClass : computer
ObjectGUID : 34760861-2aad-4d14-bca0-c16e18b05936

PS C:\Users\Administrator> Get-ADObject -Filter (distinguishedName -eq "OU=Manufacturing\0ADEL:356ed044-adf2-4035-a4c7-ee383742a8cf,CN=Deleted Objects,DC=acme,DC=com") -IncludeDeletedObjects -Properties lastKnownParent

Deleted : True
DistinguishedName : OU=Manufacturing\0ADEL:356ed044-adf2-4035-a4c7-ee383742a8cf,CN=Deleted Objects,DC=acme,DC=com
LastKnownParent : OU=North America,OU=ACME Users,DC=acme,DC=com
Name : Manufacturing
ObjectClass : organizationalUnit
ObjectGUID : 356ed044-adf2-4035-a4c7-ee383742a8cf

PS C:\Users\Administrator> _
```

Using the Recycle Bin PowerShell cmdlets in Windows Server 2008 R2 to retrieve a list of recently deleted computer objects.

Upgrades Required

Also, this new “deleted” state depends on changes made to Active Directory in Windows Server 2008 R2 – meaning you can’t leverage this new feature until *every domain controller* has been upgraded to this new version of Windows. You also have to upgrade *every domain* in your environment to the Windows Server 2008 R2 functional level, and upgrade your forest to the

Windows Server 2008 R2 functional level. That's a serious commitment for most organizations, requiring planning, new software licenses, and a significant amount of effort in order to reduce the risk of outages in a production environment.

Caution: One-Way Road Ahead

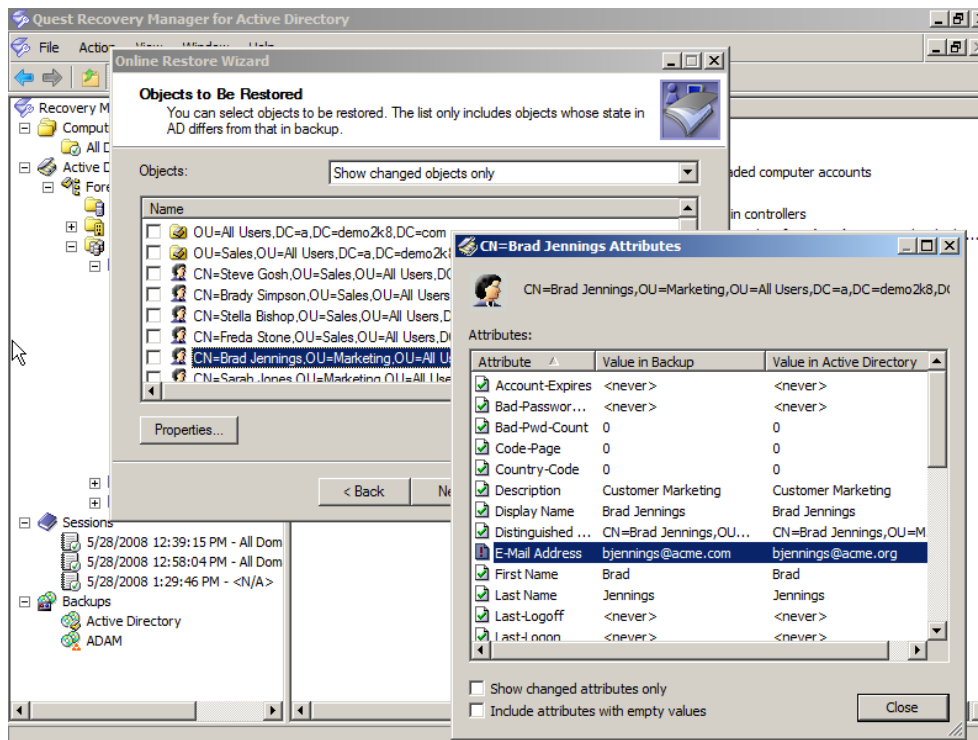
But wait, there's more to do: Once your domain controllers, domains, and forests are upgraded, you have to manually enable the Active Directory Recycle Bin functionality in Active Directory. Once you've done that, you can start writing scripts that actually let you recover deleted objects with their attributes intact. Oh, and once the Active Directory Recycle Bin functionality is turned on, you can't turn it off. So before enabling it, make *absolutely certain* that this new feature won't be in violation of any internal security rules, legislative security requirements, or industry security requirements. For example, in many European countries, it's illegal to retain personally identifiable information (PII) in certain circumstances; enabling the Active Directory Recycle Bin may unacceptably retain PII without you realizing it, since object attributes aren't deleted.

THIRD-PARTY ACTIVE DIRECTORY RECOVERY TOOLS

Third-party recovery tools, such as Quest Recovery Manager for Active Directory, work a bit differently. They typically work by making actual backups of the directory database, rather than requiring deleted information to clutter up the production database. A recovery operation might start with a comparison, which allows you to compare the current state of the directory to any past backup, automating the process of finding missing objects (there's nothing more embarrassing than restoring *most* of an organizational unit, but somehow overlooking the users who will complain the loudest that they still can't get back to work).

What About *Changes*?

In fact, *deleting* isn't the only reason you might need to initiate a recovery process: *Changes* to objects' attributes often cause more problems, and the Windows Server 2008 Active Directory Recycle Bin can't help you roll back changes. The right recovery tool can because it relies on actual data backups. This means you can quickly and easily identify changes at an attribute level, and restore any attributes which were improperly changed – on a single object, or on dozens – without taking any domain controllers offline.



Recovery Manager for Active Directory can restore individual attributes, such as account settings, group memberships and binary attributes, even when the object itself has not been deleted. This enables administrators to restore only the required attributes without affecting other attributes.

Recovering Multiple Objects or a Hierarchy?

If a deletion does occur, tools like Recovery Manager for Active Directory can make restoration much faster. With the R2 Active Directory Recycle Bin, you'll have to manually hunt down every deleted object: Leaf objects like users, but also parent objects like organizational units (OU), child OUs, and more. Recovery Manager makes it all a one-click operation, restoring the highest-level OU *and*, if you want, all the child OUs, users, computers, printers, contacts, and so forth. You can literally restore hundreds of objects in moments; with the Active Directory Recycle Bin you'll be tracking objects down (you *do* know their full Distinguished Names, right?) and writing scripts to restore them, one at a time, for quite some time.

What About Group Policy Objects?

The new Active Directory Recycle Bin functionality *only* works on objects that actually live in Active Directory – and that doesn't include those mission-critical Group Policy objects (GPOs), which live on disk. How fun is it to manually re-create an accidentally deleted – or accidentally changed – GPO? Recovery Manager recognizes that GPOs are important, integral parts of Active Directory, and includes them in its backups for easy recovery in just minutes.

Worried About Your Forest?

The new Active Directory Recycle Bin feature depends on Active Directory actually being operational. If something goes wrong with your entire *forest*, you may not even have a functional directory to work with – and even if you do, manually recovering an entire forest is a tricky task. Recovery Manager for Active Directory Forest Edition supports *complete* recovery of Active Directory, including the recovery of an entire forest and every domain within it. This is true disaster recovery.

CONCLUSION: THE NEW ACTIVE DIRECTORY RECYCLE BIN VS. THIRD-PARTY RECOVERY TOOLS

It's fantastic that Microsoft is continuing to recognize the operational needs of its customers by providing the new Active Directory Recycle Bin functionality in Active Directory. If your organization's security policies make it possible to permanently enable this feature, then you'll have the ability to recover objects and all of their attributes after accidental deletion – assuming you can write the necessary scripts, or use low-level editing commands, to actually perform the recovery.

That's why third-party Active Directory recovery tools, like Quest Recovery Manager for Active Directory and the Forest Edition, will continue to have a strong life with Windows Server 2008 R2 and beyond:

- You get a convenient, easy-to-use graphical user interface to initiate recovery operations
- You can roll back *changes*, not just deletions
- You can recover a single object, dozens, or an entire hierarchy of hundreds of objects in just minutes
- You can compare the current directory state to any past directory backup to spot changes and deletions quickly and easily
- GPOs are also protected, helping provide a more complete disaster recovery solution
- Even entire domains and forests can be recovered, ensuring that your organization is fully covered in the event of a disaster

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. For applications, we deliver, manage and control complex application environments from end-user to database. For databases, we improve performance, availability and manageability from design through production. For Windows, we simplify, automate secure and extend your infrastructure. And for virtual environments, we help you automate and control virtual desktop and server environments to reduce costs and simplify ongoing management. 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 Software can be found in offices around the globe and 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