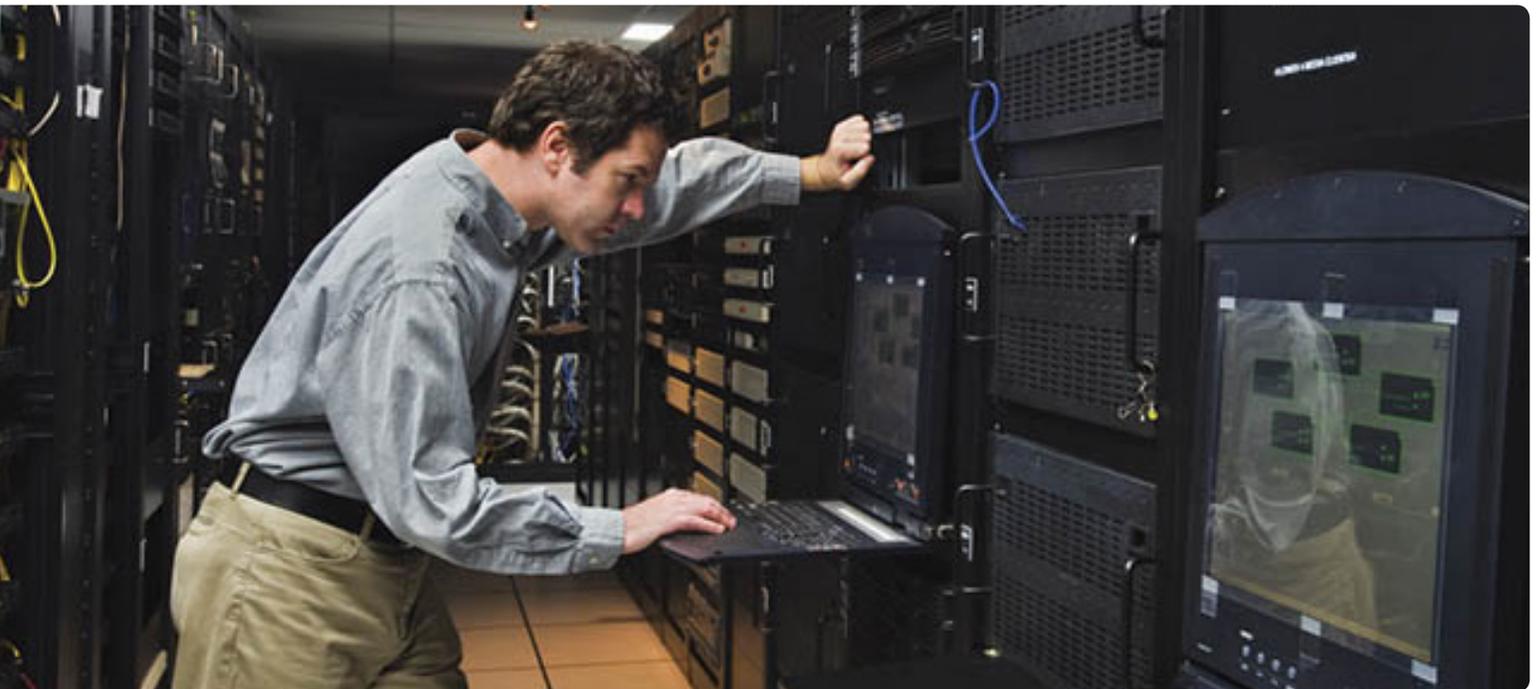


# Securing Active Directory:

An Ounce of Prevention or a Pound of Cure?



## Abstract

This technical brief reviews three tasks that should be a part of your proactive Active Directory (AD) security routine:

- Establishing levels of AD administrative security
- Auditing AD privilege use
- Remediating AD misconfigurations

As we'll see, accomplishing any of these tasks using native tools can be a difficult, manual task. But Dell® Active Administrator™ makes it easy to proactively ensure the security of your AD environment.

## Introduction

Pop quiz: Is your Active Directory secure?

And not in the "Not everyone is a Domain Admin" sense. Can you say your Active Directory is really secure?

Seems like a simple question, but odds are your answer lies somewhere between "sort of" and "not sure." Even as Active Directory has now entered its teenage years, many environments haven't matured their AD. In far too many situations, AD's basics got set up years ago but its security issues don't get addressed until after they arise.

You've heard the old adage, "An ounce of prevention is worth a pound of cure." It rings true with AD security. It takes far less work to proactively establish AD security than to clean up a mess after it happens. So considering the pounds you'd prefer to shed, let's review three tasks that should be a part of your proactive ounce of AD security:

- Establishing levels of AD administrative security
- Auditing AD privilege use
- Remediating AD misconfigurations

The Delegation of Control Wizard does not enable you to document what you've delegated.

### Task #1: Establishing levels of Active Directory administrative security

Keeping the Domain Admins group under wraps is one thing, but Domain Admin is only the topmost layer of administrative control. Even small environments have multiple admins, plenty of servers and organizational units (OUs), varying levels of responsibility, and more than a few one-off delegations. Combine these together and anyone would quickly lose track of who has what rights.

And the problem only gets worse: Add regulatory compliance and best practice standards and you're not just lost in the permissions maze; you're one mistake away from a security sit-down meeting and an RPE<sup>1</sup> or CLM<sup>2</sup> on your permanent record.

The preventative AD security strategy centers on implementing standard sets of permissions. When you establish standards, permissions can be applied repeatedly and uniformly. Doing so makes delegating

administrative security in AD as proactive as possible. But how does one standardize permissions?

Pound of cure:

#### Delegation of Control Wizard

Windows Server's Delegation of Control Wizard (DoCW), shown in Figure 1, exposes a way to establish consistent permissions for AD objects. This tool is comprehensive. At first glance, you'll find granularity in how much you can customize Active Directory permissions.

Granularity is good, right?

Not exactly. Granularity can cause complexity, especially since documentation isn't part of the Windows native package. Compliance standards and good security practices dictate that you document what you've delegated. Once you've completed a delegation with the DoCW, there is no easy way to see what you've done. Documentation, then, becomes a pencil-and-paper exercise.



Figure 1. Windows Server's Delegation of Control Wizard lets you granularly delegate custom permissions on objects

<sup>1</sup>The dreaded "Resumé Producing Event," yikes!

<sup>2</sup>A perilous "Career Limiting Move," oy!

Here's a scary example: Try delegating the resetting of passwords with the DoCW. The result isn't a single assignment but instead an adjustment to three separate permissions (Reset Password, Read pwdLastSet and Write pwdLastSet). Start adding custom delegations with specific permissions on special object types and attributes, and things get real ugly, real fast.

**Ounce of prevention:  
Dell Active Administrator**

Active Administrator from Dell provides organizations with a quick, consistent way to assess security and delegate administrative roles (see Figure 2). The solution provides all the tools you need to consistently delegate administrative control throughout your organization. You can quickly create and manage sets of permissions to be applied to objects in AD.

Active Administrator offers the following advantages over the Delegation of Control Wizard:

- Active Administrator makes it easier to define custom administrative roles.
- Active Administrator includes self-healing templates that can repair and remove unauthorized delegations.

- Active Administrator provides a color-coded indication of inherited permissions, default permissions and permissions applied with Active Administrator's Active Template technology.
- Active Administrator offers comprehensive searching and reporting to see which administrators have rights and what those rights are.

**Task #2: Auditing AD privilege use**

Let's now assume you've established AD permissions consistently. Groups are created, delegations are assigned, and everything's humming along nicely. How do you ensure that AD permissions are delegated properly?

**Pound of cure:  
Auditing event logs with native tools**

With native tools, ensuring that AD permissions are delegated properly is a challenge. You must watch carefully and compare the exercise of permissions against what you think you've delegated. That means generating audit logs and manually comparing those audit logs against the documentation you created (with pencil and paper) in Task #1.

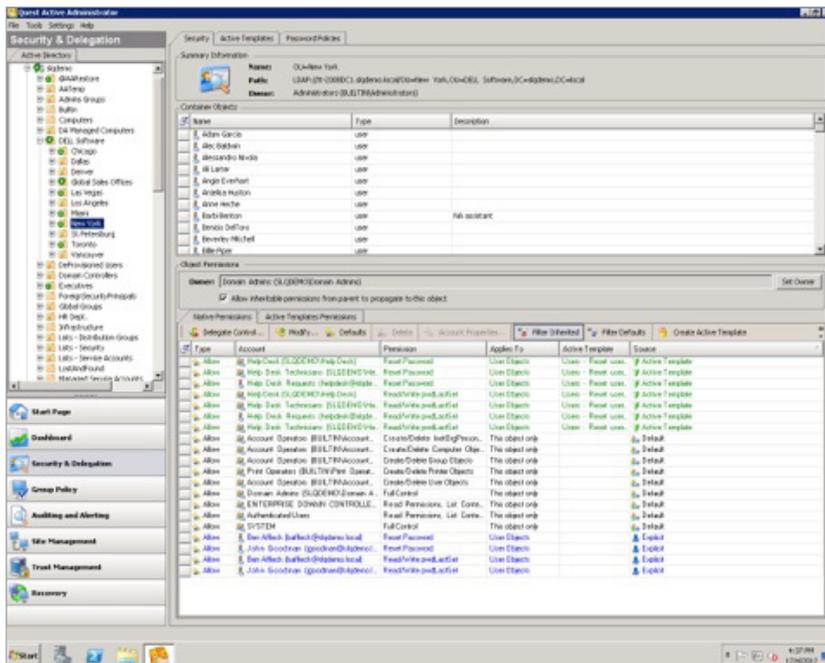


Figure 2. Assessing AD administrative security is easy with Active Administrator.





Admittedly, Windows Server has some nice AD auditing features. For example, Event Log Forwarding can consolidate event logs from multiple servers. This feature works great for very small environments, but it doesn't scale well past a few servers with a few events.

Windows can also automatically run a scheduled task when a previously configured event occurs. Set that task to send an email to yourself, and you've got the beginnings of an audit alert system.

For instance an Active Directory password change will generate, among other events, an Event ID 4738. Knowing this, you can configure Windows Server to email you whenever an Event ID 4738 event is generated; just assign an email task to the specific Event ID, source and log.

But consider all the events that require attention. For any action taken by someone managing AD, you've got a new Event ID to audit. More actions mean more audits, which means more tasks to generate and manage. For an operational AD domain, you'll need to monitor a myriad of object creation, modification and deletion events—in some cases down to the attribute level—for specific sets of objects. Doing so requires creating a complex mixture of custom views which require periodic

manual review as part of your regular maintenance.

It seems the native "solution" is really a pound of cure in disguise.

### Ounce of prevention:

#### Active Administrator

Active Administrator, on the other hand, enables you to quickly and accurately recognize changes in Active Directory. An audit agent actively monitors the security of event logs on each domain controller where it is installed. Upon finding an event of interest, the audit agent sends the information to the auditing database.

With Active Administrator, you can:

- Create, organize, save and export out-of-the-box and custom reports
- Filter data in reports by date/time range, acting user, event type, object type and more
- Schedule reports for delivery
- Receive alerts when specific AD events occur
- Configure actions to run automatically when certain AD events occur

The biggest difference between Active Administrator and using native tools to audit event logs is the sheer convenience and ease of Active Administrator—it offers a straightforward, automated approach to monitoring AD events.

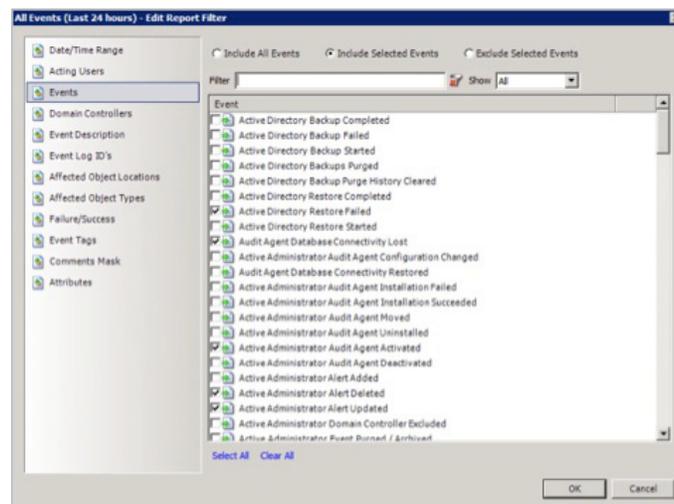


Figure 3. Filtering for AD events with Active Administrator



### Task #3: Remediating AD misconfigurations

With multiple administrators managing AD together, even the best laid configurations often go astray. Remediating AD configurations can be challenging: First, you must figure out who has rights to manage the modified object in question; then you must work backward through the myriad of nested OUs and groups to find the source of the rogue configuration.

There is a better way. True remediation demands automation: a solution that will notify you when something goes awry and offer to fix the problem automatically.

#### Pound of cure: Remediating AD misconfigurations with native tools

Windows Server 2008 R2 and Windows Server 2012 include a vastly expanded set of auditing categories. While earlier versions had nine categories, these versions have some 50 additional auditing subcategories.

One important subcategory for finding maladjusted permissions is Audit Active Directory Service Changes, found under the traditional DS Access category. Figure 4 shows where this subcategory can be enabled using Group Policy. This subcategory is unique in that it monitors for changes made to objects

in Active Directory. When a change is found, the old and new values of the changed object property are captured in the event log.

As with the other tasks, this functionality might appear to be a good solution at first blush. Dig just a bit deeper into its inner workings, however, and the native tools for getting data back out might involve more effort than reward.

Directory Service Change events are captured in the audit log in a Windows domain controller's event viewer. This happens to also be where all other events of all types get captured. As a result, even in a very small environment, you might be forced to mine through tens or hundreds of thousands of entries to find a notable change.

Audit events with this subcategory are also only logged for objects with configured system access control lists (SACLs), and only when they are accessed in a manner that matches their SACL settings. Therefore, some objects and properties will not cause an audit to be generated. Getting around this limitation requires a careful coordination of object monitoring using some of Windows' most dangerous tools—those where an errant mouse click can have the greatest impact on AD operations.

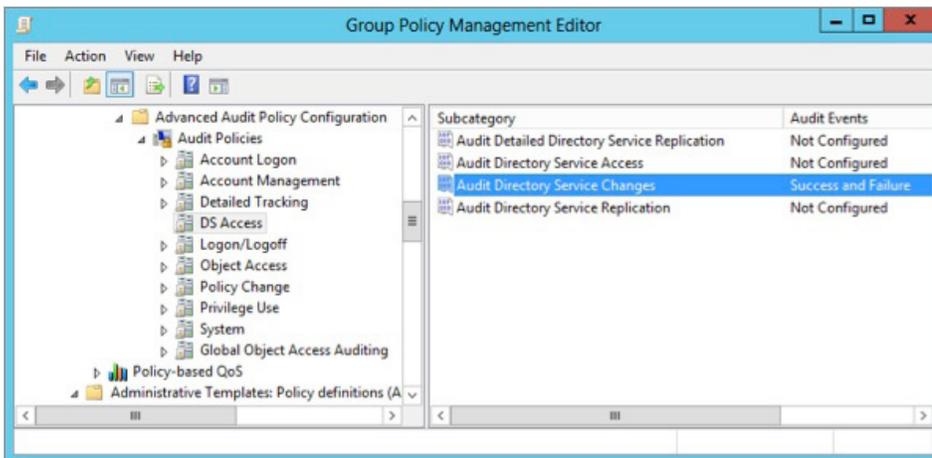


Figure 4. Windows Server now includes some 50 auditing subcategories.

## Ounce of prevention:

### Active Administrator

In addition to streamlining delegation and auditing AD events, Active Administrator also provides the ability to restore AD objects to a previous state (which includes security). Active Administrator can back up Active Directory twice a day and enables you to recover GPOs, entire AD objects, object attributes and object security. Active Administrator's broad AD management capabilities offer a blended approach to remediating AD misconfigurations in a customized, proactive way.

### Conclusion

Staying clear of the "pound of cure" requires an ounce of prevention—and implementing the right ounce is perhaps

the most important decision you'll ever make. Native tools get you only so far. Active Administrator delivers the complete automation and flexible granularity you need to best manage your AD security.

The smart move? Save yourself that security sit-down meeting. Take a hard look at the entire solution your Active Directory needs for heavy-duty security, and remember that an ounce of prevention is worth a pound of cure.

For more information about Active Administrator, visit [quest.com/active-administrator](http://quest.com/active-administrator).

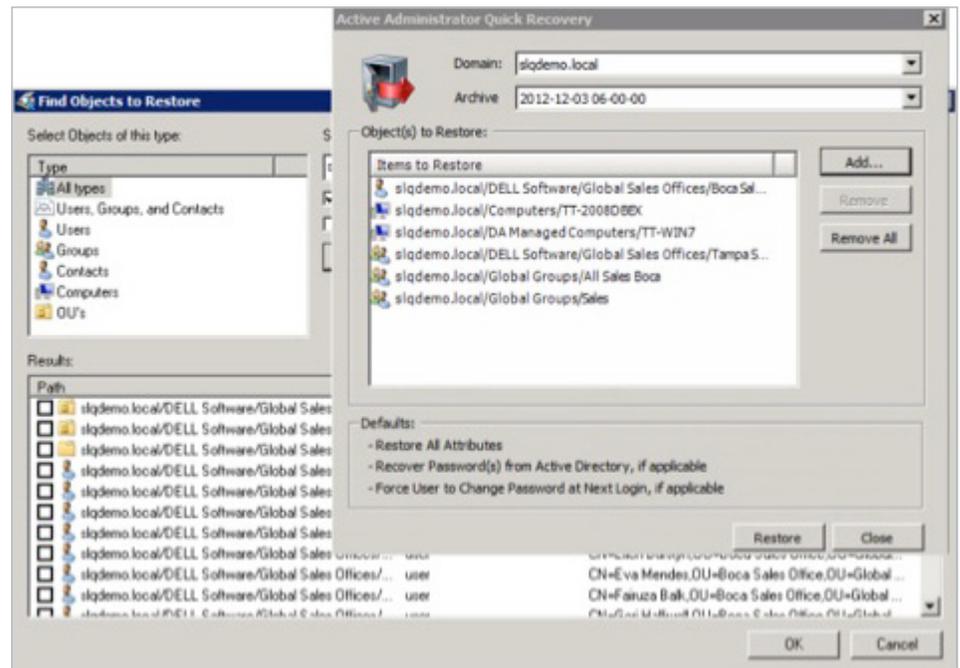


Figure 5. Recovering AD objects is easy with Active Administrator.

## For More Information

© 2013 Dell, Inc. ALL RIGHTS RESERVED. This document contains proprietary information protected by copyright. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose without the written permission of Dell, Inc. ("Dell").

Dell, Dell Software, the Dell Software logo and products—as identified in this document—are registered trademarks of Dell, Inc. in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with Dell products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Dell products. EXCEPT AS SET FORTH IN DELL'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT,

DELL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell does not make any commitment to update the information contained in this document.

## About Dell

Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit [www.dell.com](http://www.dell.com).

If you have any questions regarding your potential use of this material, contact:

## Dell Software

5 Polaris Way  
Aliso Viejo, CA 92656  
[www.dell.com](http://www.dell.com)

Refer to our Web site for regional and international office information.

