Active Directory Auditing: What It Is, and What It Isn't

Abstract

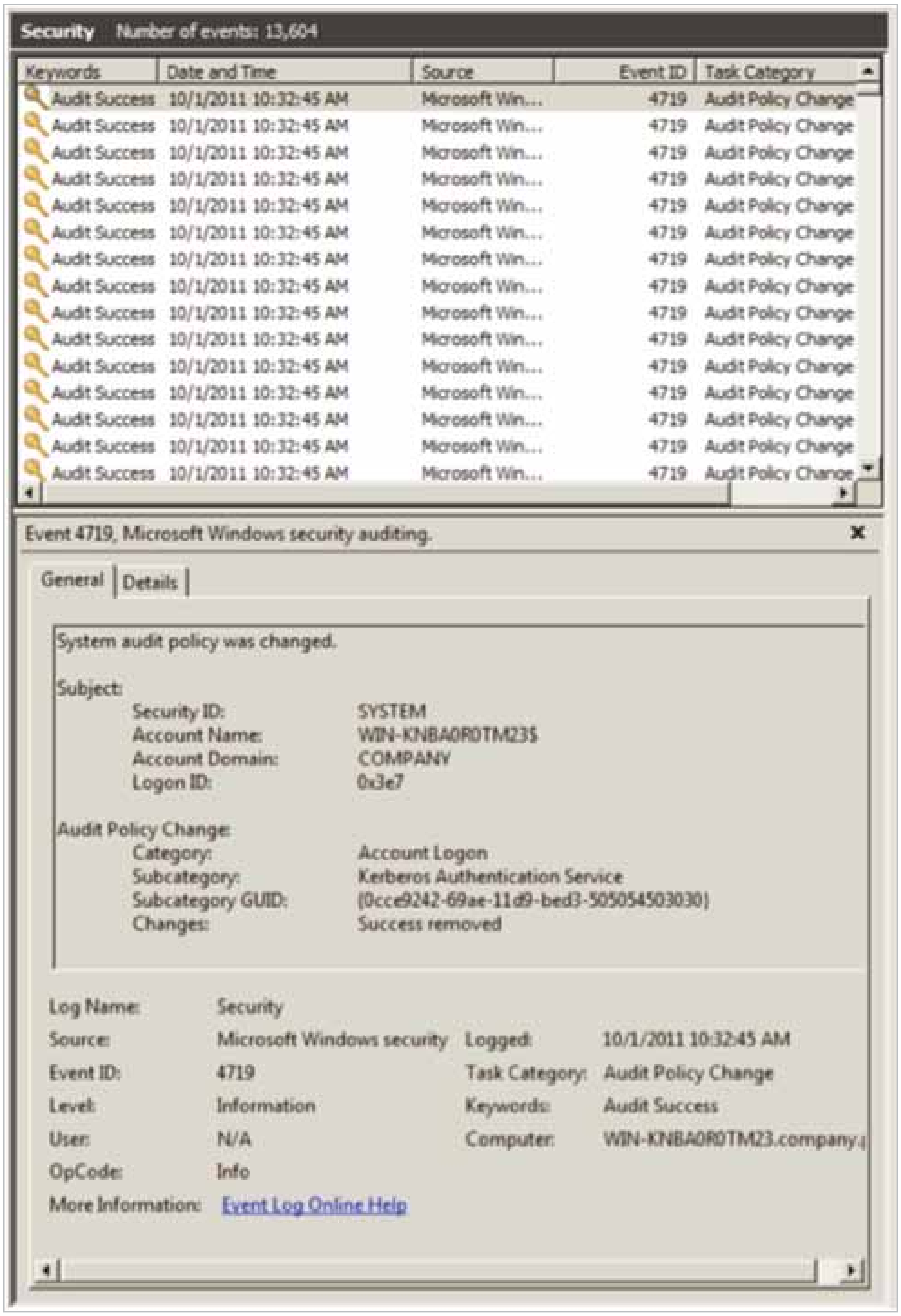
What's wrong with Active Directory's native audit logging? More importantly, what functionality do you really need in an AD auditing solution, and where can you find those capabilities? This white paper explains it all.

At a recent TechEd discussion, attendees agreed that auditing was a balance between “what the organization wants, and what it’s willing to pay for.”

Introduction

Let’s talk about auditing in Active Directory. Figure 1 shows what the native tools give you.

Lots of data there. Not so much information. We can see that the “Success” audit policy for account logons was removed. We can see that logon ID 0x3e7 made the change. Riiiight. We’ll have to look that up later. But you know, we can see what was changed. Cool. But gosh, there’s so much more you might



Security Number of events: 13,604

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	10/1/2011 10:32:45 AM	Microsoft Win...	4719	Audit Policy Change
Audit Success	10/1/2011 10:32:45 AM	Microsoft Win...	4719	Audit Policy Change
Audit Success	10/1/2011 10:32:45 AM	Microsoft Win...	4719	Audit Policy Change
Audit Success	10/1/2011 10:32:45 AM	Microsoft Win...	4719	Audit Policy Change
Audit Success	10/1/2011 10:32:45 AM	Microsoft Win...	4719	Audit Policy Change
Audit Success	10/1/2011 10:32:45 AM	Microsoft Win...	4719	Audit Policy Change
Audit Success	10/1/2011 10:32:45 AM	Microsoft Win...	4719	Audit Policy Change
Audit Success	10/1/2011 10:32:45 AM	Microsoft Win...	4719	Audit Policy Change
Audit Success	10/1/2011 10:32:45 AM	Microsoft Win...	4719	Audit Policy Change
Audit Success	10/1/2011 10:32:45 AM	Microsoft Win...	4719	Audit Policy Change
Audit Success	10/1/2011 10:32:45 AM	Microsoft Win...	4719	Audit Policy Change
Audit Success	10/1/2011 10:32:45 AM	Microsoft Win...	4719	Audit Policy Change
Audit Success	10/1/2011 10:32:45 AM	Microsoft Win...	4719	Audit Policy Change
Audit Success	10/1/2011 10:32:45 AM	Microsoft Win...	4719	Audit Policy Change
Audit Success	10/1/2011 10:32:45 AM	Microsoft Win...	4719	Audit Policy Change

Event 4719, Microsoft Windows security auditing.

```
System audit policy was changed.

Subject:
        Security ID:          SYSTEM
        Account Name:         WIN-KNBA0R0TM23$
        Account Domain:       COMPANY
        Logon ID:             0x3e7

Audit Policy Change:
        Category:             Account Logon
        Subcategory:          Kerberos Authentication Service
        Subcategory GUID:     {0cce9242-69ae-11d9-bed3-505054503030}
        Changes:              Success removed
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	10/1/2011 10:32:45 AM
Event ID:	4719	Task Category:	Audit Policy Change
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	WIN-KNBA0R0TM23.company.
OpCode:	Info		
More Information:	Event Log Online Help		

Figure 1. Native tools provide lots of data, but not much information

want to know. "Who made the change?" would be a good start, for example.

And you know, you would have found this event only after digging for a bit, because it would be logged only on the domain controller where the change was made, right? How many DCs would you have to search through to find any given event?

This actually just scratches the surface of what's wrong with Active Directory's native audit logging. Let's look at the full list:

- It's distributed. Want to find a problem? You'll have to look at every server's log. In Windows Server 2008 R2, you can configure event forwarding, which will at least consolidate all of the entries into one server's log, but you'll also need to do some performance and capacity planning on that.
- It's intense. Crank up AD auditing to the max level, and be prepared to deploy some new DCs to help pick up the workload. In fact, at a recent TechEd discussion, attendees agreed that auditing was a balance between "what the organization wants, and what it's willing to pay for," because more information equals more workload, which equals more servers to spread the workload across.
- It's not English. Out of the entire log entry above, only a handful of data points are immediately useful. The rest are going to require lookups and cross references to make sense of.
- It's not secure. Any administrator can wipe the log, and it's not even too hard to do by accident. Yes, a message is left behind saying that they did it, but the stuff they erased is gone forever.
- It's a lot. The native filtering and searching capabilities are okay, but because the logs aren't consolidated and because they don't always contain plain-English information, it's sometimes difficult to use the filtering feature to actually find anything useful.
- It's administrator-only. At least, you're not likely to want your auditors, or anyone else, browsing around inside Server Manager, looking at events. But there's no other way to deliver that information to them – no built-in reporting of any kind.

One solution is to use the Microsoft Audit Collection Service, or MACS. It's designed to consolidate Security Log entries, in near-real-time, into a SQL Server database that can be independently secured, and which is more easily queried and searched than the native event logs. Great idea – except that MACS is available only as part of System Center Operations Manager, which isn't exactly cheap, nor easy to just set up and run. MACS also won't give you reporting, although getting the information into SQL Server at least opens up the possibility of custom-building reports using SQL Server Reporting Services. Sound fun? Didn't think so.

What do you need in auditing, anyway?

If you're going to be shopping for a better approach to auditing, take a minute to think about what you might actually need. Here's a wish list to get you started:

- Consolidated. One log, for the entire domain. Period.
- Secure. Above all, you want the audit log to be separated from administrator privileges. They shouldn't be able to clear it on a whim, or deliberately, or by accident.
- Performance. Capturing detailed auditing information shouldn't bring a DC to its knees. There's always going to be a compromise between information and performance, but you should be able to strike a good balance.
- Live View. Sometimes you need to see what's going on right now, or what's just recently happened. There should be a way to do that without having to click "Refresh" or open a dozen console windows to different servers.
- Detail. When was the change made? Where? Who made it? What was changed?
- Filters. We're always going to have tons of events in the logs; what's needed is a way to intelligently – and quickly – filter them down, based on the users involved, or time ranges, or by objects (or object types) affected.
- Reports. What about being able to run actual reports from the audit log, and perhaps being able to have those

If you can get your logs into a database–in close to real-time–then you'll get pretty much everything you need from those logs, including all seven of those desirable capabilities.

automatically emailed as PDF or XLS files on a scheduled basis? Man, the auditors would love that.

You may have some other criteria, but odds are that this list of seven key capabilities will cover what most organizations need from their auditing. Looking at those seven capabilities, you'll find one common underlying technology that can pretty much deliver them all: a new-fangled thing called a database. Yes, it's that simple! If you can get your logs into a database – in close to real-time – then you'll get pretty much everything you need from those logs, including all seven of those desirable capabilities.

You see, Windows' log files aren't stored in a database. They're stored in something a lot more like a text file, which is what makes them lower-performance and more difficult to secure, search, filter, and report on. But if those events were being copied into a live, relational database, then you'd get all the features that we normally associated with databases: speedy queries, fast searching, quick filtering, and more. You'd also get the ability to secure that database independently of the native log files.

It's the database in Active Administrator–plus its intuitive user interface –that makes the difference.

Of course, a database isn't the complete answer. You also need intelligence. Like the guy who's been working with Windows since Windows NT 3.1, who's memorized the event ID numbers, who can translate hexadecimal in his head, and who knows the security ID (SID) of every object in the domain.

Actually, that kind of a guy would probably be creepy.

Getting the seven key capabilities

Active Administrator handles all seven of the key capabilities we identified, and then some. In addition to superior Group Policy management, point-and-click recovery capabilities, and centralized management of permissions and delegation, Active Administrator has truly effective auditing for Active Directory.

- Use Live View to see what's happening, right now, in your directory, including the "who, what, where, and when" details that you need. Create reports that include specific criteria for the events you want to see, and then run those reports whenever you want to – or even schedule them for automatic delivery to whoever needs them. Auditors will drool.
- Use nine different filter criteria to narrow down the massive event log into just the events you want to see.
- Best of all, events are consolidated in near real time into a SQL Server instance, which can be independently secured and protected to create a truly tamperproof audit trail.

It's the database in Active Administrator – plus its intuitive user interface – that makes the difference. It's fast because it's based on real database technologies, not on just consolidating text files into another text file. Layer on its management interface and you've got a speedy, powerful tool that lets you work with event logs in ways you've probably never imagined.

Active Administrator also brings the event log intelligence you need – without any creepy guys. It knows how to translate event information into plain English, so you're not left wading through hex code, translating SIDs, and so forth. The most difficult information gets translated for you, making those events not only easier to find, but easier to read – and easier to take action upon.

Why not see for yourself? At www.quest.com/active-administrator, you can play with Active Administrator in a live, online TestDrive, or download a trial to try it in your own environment. A complete product walkthrough will show you want to expect and outline its other cool features. Get started today!

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.

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