Windows® IT Pro

7 Tips for Achieving Active Directory Compliance

By Darren Mar-Elia

QUEST SOFTWARE®
Simplicity At Work™

→ Contents

7 Tips for Achieving Active Directory Compliance..2

Introduction...2

The Ups and Downs of Native AD Auditing 2

The Ups!..3

The Downs 4

Auditing and Compliance in AD..............6

Leveraging Third-Party Auditing Tools.......7

What to Look for, and What to Look Out for..7

Conclusion 8

About the Author 8

Appendix: Quest Solutions for Compliance..9

7 Tips for Achieving Active Directory Compliance

By Darren Mar-Elia

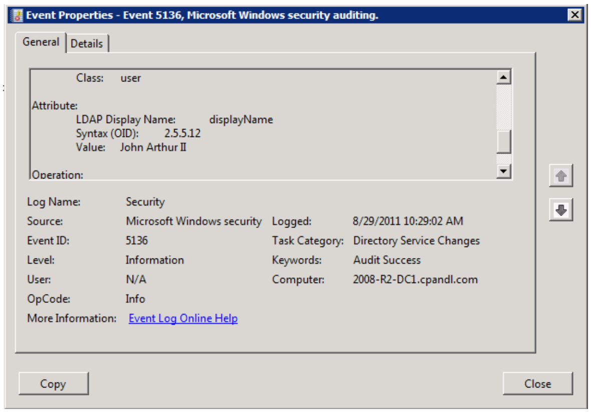
Introduction

In many organizations, Active Directory (AD) is a key point of authentication and authorization to important corporate resources. As a result, the user identities stored in AD and the groups they are members of are important points of control and audit for knowing what is being accessed within your organization. The ability to audit and be alerted about changes to AD is a critical part of any organization.

The native auditing with AD can meet some, but not all, of your auditing and compliance needs. In this paper, I'll provide tips and tricks to make the best use of native AD auditing, as well as guidelines on what auditors and compliance officers look for when it comes to keeping an eye on what's going on within your AD environment. I'll also look at some third-party alternatives to native auditing that can greatly enhance your ability to fully report on what's happening within your AD infrastructure.

The Ups and Downs of Native AD Auditing

The ability to audit what is going on within your AD infrastructure has evolved over the years—going from really limited in Windows Server 2000 and 2003 environments to pretty good in Server 2008 and 2008 R2 environments. The main challenge with AD auditing in those earlier versions of Windows was that a) not all changes to AD were logged or logged in a way that was useful and b) before and after values of changes were not logged at all, so you had no way of knowing what the old data was unless you restored the object from backup. With the release of Server 2008 and then Server 2008 R2, native AD auditing got better. Those releases offer more complete coverage of audited events, and before and after values of modified attributes are now captured in the Windows security event log (see Figure 1), albeit within two separate events: one that records the original value of the attribute and another that records the new value.


Event Properties - Event 5136, Microsoft Windows security auditing.
General
Details
Copy
Close

Class: user

Attribute:
LDAP Display Name: displayName
Syntax (OID): 2.5.5.12
Value: John Arthur II

Operation:

Log Name: Security
Source: Microsoft Windows security
Logged: 8/29/2011 10:29:02 AM
Event ID: 5136
Task Category: Directory Service Changes
Level: Information
Keywords: Audit Success
User: N/A
Computer: 2008-R2-DC1.cpandl.com
OpCode: Info
More Information: Event Log Online Help

Figure 1: Viewing changed values in Server 2008 R2 AD

The Ups!

Let's take a look at how auditing works in AD and how you can enable the right auditing on your AD objects. For my examples, I'll be using Server 2008 R2. I will make note of any significant differences that exist between this newest version of Windows Server and earlier versions.

The first thing to know about enabling AD auditing is that there is no single button to push to turn on all the auditing you might need. Instead, it's a multi-step process:

1. The first step involves telling an AD domain that you want to enable auditing (and which categories you want to audit).

2. The second step involves setting the Security Access Control List (SACL) on a particular object or objects to let AD know which objects you want to see audit events for.

Step 1. Tell the AD domain that you want to enable auditing

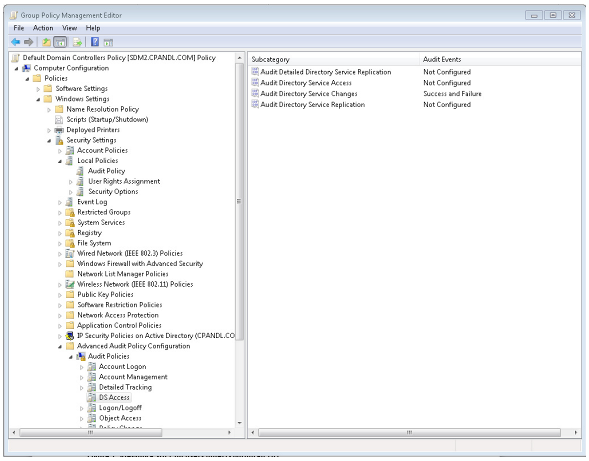
Let's look at the first step. Being able to audit AD events requires telling all your domain controllers that they should pay attention to any changes that happen to AD. This involves enabling some Group Policy settings within your AD domain.

In Windows Server 2003, you had only one level of granularity in terms of AD auditing: it was either all on or all off. The standard procedure for this was to open the Group Policy Editor, focus on the "Default Domain Controllers Policy" Group Policy Object (GPO), and enable the **Directory Service Access** audit policy under Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy. Once this audit policy was enabled for success or failure events, then any AD objects that had a SACL configured to audit changes would send change events to the security event log on the domain controller (DC) that **originated the change**. This is an important point!

TIP #1: **AD changes are logged only within the security event log on the DC that originated that change. In other words, AD does not replicate security events to all DCs the way it replicates object changes!**

Starting in Windows Server 2008, you now have the ability to set more granular auditing of AD events, differentiating between AD changes, AD access events (events related to people accessing AD), AD replication operations, and detailed AD replication. These four subcategories give you more granularity over what is logged within the Windows security event log, and thus more control over the volume of security events that are being logged.

TIP #2: **In Server 2008, these subcategories are exposed through the *auditpol.exe* command-line utility. However, in Server 2008 R2, you can now enable and disable these sub-categories through Group Policy, under Computer Configuration\ Windows Settings\Security Settings\Advanced Audit Policy Configuration (see Figure 2).**

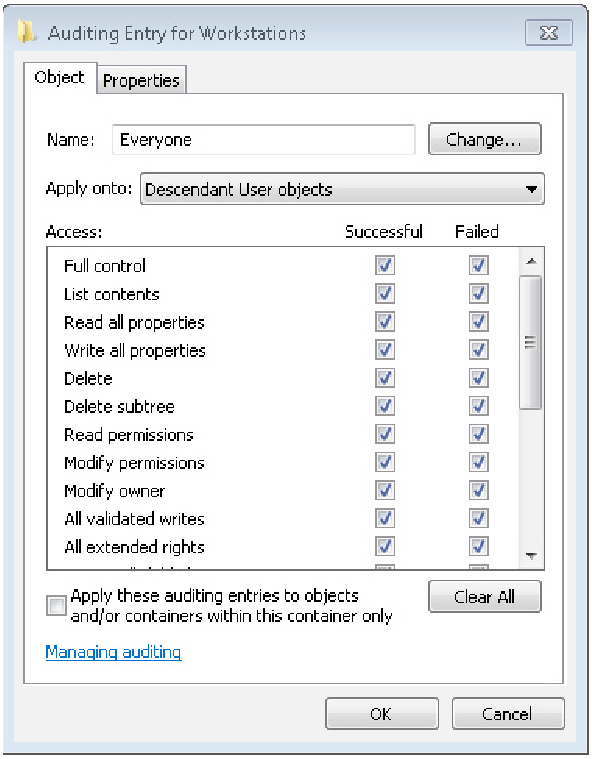

Group Policy Management Editor
File
Action
View
Help
Default Domain Controllers Policy [SDM2.CPANDL.COM] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Directory (CPANDL.CO
Advanced Audit Policy Configuration
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access

Subcategory	Audit Events
Audit Detailed Directory Service Replication	Not Configured
Audit Directory Service Access	Not Configured
Audit Directory Service Changes	Success and Failure
Audit Directory Service Replication	Not Configured

Figure 2: Viewing Advanced Audit Policy Configuration in Group Policy

Step 2. Let AD know which objects you want to see audit events for using the SACL.

Once auditing is globally enabled in an AD domain, the next step is to ensure that the objects you are interested in tracking within AD have the correct SACL to allow for auditing events to be generated against them. The SACL on a given AD object or objects is accessible from the "Advanced" tab within the typical ACL Editor within AD Users & Computers (or similar tool). When you define a SACL, much like when you define a standard Access Control List (ACL), you specify which user or group you are interested in auditing against. In other words, if you want to track changes against a given AD object by a specific person, you would add that person's user ID to the SACL, along with whether you want to audit success or failure changes and what properties and object classes you want to audit against. Figure 3 shows a typical SACL for user objects that was defined at an OU level.



Name: Everyone

Apply onto: Descendant User objects

Access:	Successful	Failed
Full control	☑	☑
List contents	☑	☑
Read all properties	☑	☑
Write all properties	☑	☑
Delete	☑	☑
Delete subtree	☑	☑
Read permissions	☑	☑
Modify permissions	☑	☑
Modify owner	☑	☑
All validated writes	☑	☑
All extended rights	☑	☑

☐ Apply these auditing entries to objects and/or containers within this container only

Figure 3: Viewing a SACL on user objects within an OU

TIP # 3: **If you want audit events to show up for all objects in your AD domain, you'll have to set up a SACL at the domain level that covers all objects and their attributes and all users (e.g., by using the Everyone group). Note, however, that this will truly mean that every change that happens to AD will be logged in the security event log on the originating DC—which for larger domains could mean a lot of events.**

When global auditing is enabled and the objects that you are interested in auditing have SACLs in place, you can expect to start getting events in the security event log of the originating DCs related to your changes. On Server 2008 and 2008 R2, these events will appear in the security event log under the **Directory Services Changes** task category.

TIP #4: **Another thing to note is that the "Directory Service Access" subcategory is also useful from a compliance perspective because it logs accesses to AD data. However, if the SACLs on your AD tree are extensive, this subcategory can generate a lot of data, so be cautious about enabling this category.**

The Downs

While there have been improvements in AD auditing with respect to the coverage and quality of audit data that is logged, when it comes to implementing enterprise auditing of AD for the purposes of satisfying audit and compliance requirements, much is still lacking.

Handling the Volume of Audit Data

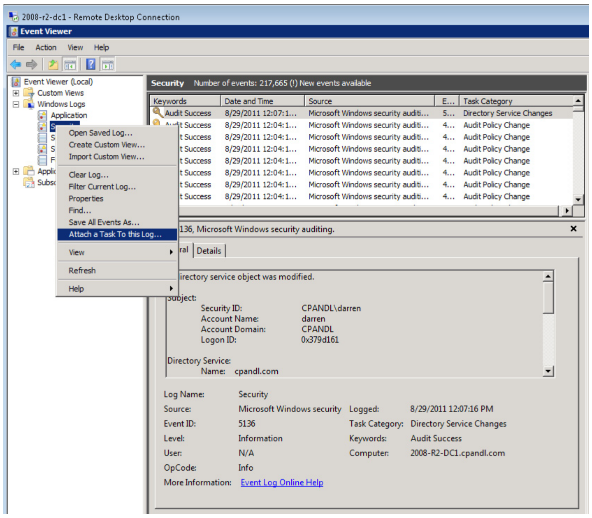
Let's start by tackling the challenge of the sheer quantity of audit data that can be generated by AD in a reasonably sized environment. In an environment of several thousand users, it's not uncommon for domain controller audit logs to roll over within a single day. In other words, unless your security logs are set to a very big size, you might not be able to see all events within a given day, because most IT shops will set their event logs to roll over as needed rather than stop logging. Of course, the security event log logs more than just AD changes—it's also logging any other security-related events enabled on your domain controllers.

This means that you will likely need to have some way of capturing and consolidating events of interest before they roll over. This is especially important if you're going to report across the enterprise for audit data that is generated, because it's very cumbersome to try to do this across multiple domain controllers. There is no simple way to do that in a scalable way out of the box. Microsoft does provide the notion of event forwarding, where you can selectively forward events from multiple systems' event logs to a single consolidated log, but the scalability on that is subject to the size of your infrastructure.

TIP #5: **You can use the Event Forwarding feature in Server 2008 and above to forward select security events from one or more DCs to a central event log. Just keep scalability in mind when you do this, because the volume of events in larger environments could outstrip this native feature's capability.**

Alerting and Reporting on Audit Events

Another key challenge is alerting and reporting on audit events. Most shops need to be able to generate a report for an auditor or be notified when a particular high-risk change occurs (such as when somebody is added to the Domain Admins group). There is no easy, scalable way to do that out of the box. You can use the built-in features to "attach a task" to a particular event log entry occurrence (see Figure 4) and then use that task to send some kind of alert (e.g., by email). But again, that won't scale to many alert types and many alerts.



Security Number of events: 217,665 (!) New events available

Keywords	Date and Time	Source	E…	Task Category
Audit Success	8/29/2011 12:07:1…	Microsoft Windows security auditi…	5…	Directory Service Changes
A…dit Success	8/29/2011 12:04:1…	Microsoft Windows security auditi…	4…	Audit Policy Change
t Success	8/29/2011 12:04:1…	Microsoft Windows security auditi…	4…	Audit Policy Change
t Success	8/29/2011 12:04:1…	Microsoft Windows security auditi…	4…	Audit Policy Change
t Success	8/29/2011 12:04:1…	Microsoft Windows security auditi…	4…	Audit Policy Change
t Success	8/29/2011 12:04:1…	Microsoft Windows security auditi…	4…	Audit Policy Change
t Success	8/29/2011 12:04:1…	Microsoft Windows security auditi…	4…	Audit Policy Change
t Success	8/29/2011 12:04:1…	Microsoft Windows security auditi…	4…	Audit Policy Change

136, Microsoft Windows security auditing.

```
irectory service object was modified.

Subject:
        Security ID:        CPANDL\darren
        Account Name:       darren
        Account Domain:     CPANDL
        Logon ID:           0x379d161

Directory Service:
        Name:   cpandl.com
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	8/29/2011 12:07:16 PM
Event ID:	5136	Task Category:	Directory Service Changes
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	2008-R2-DC1.cpandl.com
OpCode:	Info		
More Information:	Event Log Online Help		

Figure 4: Attaching a task to an alert to generate alerts on security events

Reporting on AD Audit Events

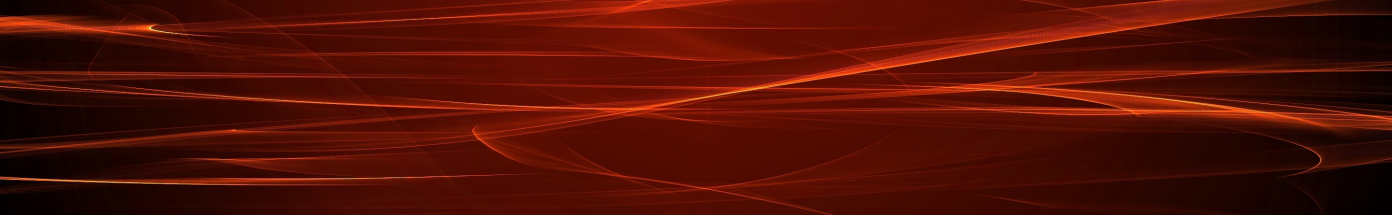
Another gap with native tools is reporting on AD audit events. Even if you're able to consolidate logs, you're going to need some way of being able to generate reports for your auditors, and that is not available with the native OS. Answering questions such as "Tell me all group membership changes that happened in the last 30 days on a given set of groups" is exceedingly difficult, if not impossible, without some kind of reporting tool in place. Further, if regulations require that you keep and archive audit logs, you need a way of doing that in an organized, structured way (other than saving off the actual event log files).

Change Auditing for Group Policy Objects

Finally, let's discuss one last key deficiency that is likely to cause you and auditors headaches: the lack of any change auditing for Group Policy Objects (GPOs). Group Policy is the configuration management feature within AD that lets you secure and configure your Windows desktops and servers en masse. GPOs are responsible for everything from your domain password policies to controlling who can log into which servers and workstations. As a result, auditors find the control and use of GPOs to be very interesting. That means that you need to have good processes in place for auditing when changes happen to GPOs. Unfortunately, the native OS is sorely lacking here. Windows Server will log when a change occurs to one of the AD "parts" of a GPO, but it will not log which settings were changed within the GPO. This means you're left knowing that *something* changed, but not knowing what the change was—not very satisfying for your typical auditor.

TIP#6: **You can see when a GPO was changed by looking for a Directory Services Change event against a groupPolicyContainer class object. This event will correspond to the AD part of a GPO and will show you limited information about who made the change and which properties on the AD part of that GPO were changed. You won't see any information related to what setting changed in the GPO, but at least you know who made the change.**

Now that we've looked at what you can do with native tools, let's talk about what auditors are typically



looking for with respect to AD and how you can make sure you're prepared for any situation.

Auditing and Compliance in AD

What Auditors Want

As I mentioned earlier, AD is a rich source of information for auditors and compliance officers. Because it controls access to so many resources in a typical environment, it's important to be able to show auditors that you know what's happening at all times within your AD environment. This means having audit logs to prove you know about all the changes and what those changes are. Some examples of changes that are of particular interest to auditors:

- Changes to group membership, especially groups that control privileged access (e.g., Domain Admins or similar) and groups that control access to sensitive corporate data (e.g., access to file servers or other data sources)
- Changes to attributes that are security sensitive (e.g., password changes) or the disabling/enabling of user or computer accounts, especially looking to see that employees who leave the organization are disabled upon leaving and that their accounts are not used for access after they've left
- Changes to audit policy that would result in auditing changes or events that indicate that security logs have been cleared
- Changes to Group Policy Objects, especially those GPOs that control security on desktops and servers (e.g., password policy)

If you're relying on native tools to get the information that auditors need, you'll need to ensure that you're not inundated with log data that would prevent you from effectively logging and keeping this kind of information. This means ensuring that you are logging the data you really need to limit the slew of event log data that can result in a typical AD environment. This means enabling only those categories of logging that are relevant to your audit and management needs. If you are running in a Server 2003 AD environment, you know that you have only very coarse control over what events can be audited (as I mentioned earlier). But if you have any 2008 or 2008 R2 DCs, you can take advantage of the subcategories of logging that are enabled through auditpol.exe or Group Policy to tune down what is collected.

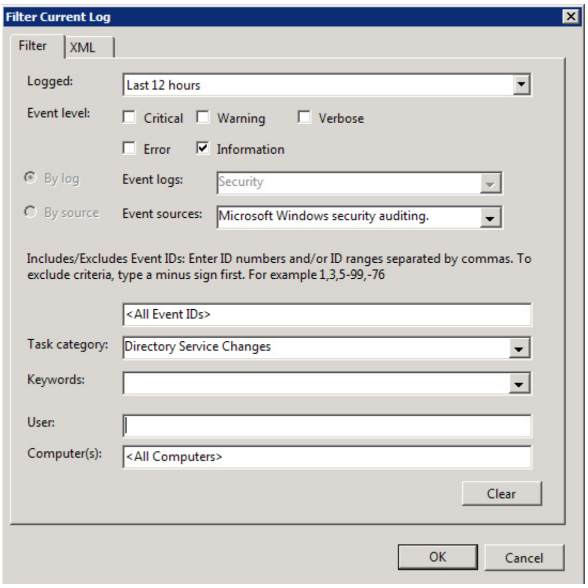
TIP #7: **Use Advanced Audit Configuration (Figure 2) or auditpol.exe on your Server 2008 or R2 DCs to only enable auditing on those subcategories you really need to meet your audit and security requirements. See http://technet.microsoft.com/en-us/library/cc731607(WS.10).aspx for more details. Also, avoid using audit categories that produce extraordinary quantities of security events (e.g., Object Access auditing), unless you are only doing it for short periods of time.**

Giving Auditors What They Want

The key to a successful AD audit is ensuring that you have the information that auditors typically need, right at your fingertips. This means making sure that you have the right auditing enabled, and that you can report on that information at a moment's notice. You don't want to be in a position where an auditor asks you to prove that no one has logged into your domain controller consoles in the last 90 days and say that you can't.

The main thing auditors want to know is that you have a coordinated process in place for changes that occur to AD and that you can prove that you know about all those changes. But they are not concerned with changes to a user's phone number (in most cases). What they most care about are changes that would grant access to critical resources or changes that circumvent good security practices (e.g., setting a user account's password to "never expire"). Because user accounts, security groups, and (to a lesser degree) computer accounts are the biggest targets for auditors, that's where you should ensure that you are logging any changes and are able to report against those for a given time period.

If you are using the event log forwarding feature I mentioned above, then you can go to a single event log to be able to query all events related to a particular account or event ID. The filtering feature within the Server 2008 event log (see Figure 5) can make this process easier because you can filter by dates, event sources, and description text within the log.


Filter Current Log

Filter | XML

Logged: Last 12 hours

Event level: □ Critical □ Warning □ Verbose □ Error ☑ Information

● By log Event logs: Security

○ By source Event sources: Microsoft Windows security auditing.

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

<All Event IDs>

Task category: Directory Service Changes

Keywords:

User:

Computer(s): <All Computers>

Figure 5: Filtering security events based on various criteria

By showing that you have a process in place around AD and Group Policy changes, and by being able to back that up with audit reports showing all changes made against critical AD objects, you will be able to meet or exceed auditor's needs for your AD environment.

But as I've described, there are some significant limitations with the native auditing, collection, alerting, and reporting that can limit your ability to report what auditors expect. For those reasons, I generally suggest that folks have a look at the third-party AD auditing products on the market because they can really make a difference in terms of your ability to quickly and easily report on AD changes.

Leveraging Third-Party Auditing Tools

Advantages of Third-Party Auditing Tools

The advantages of third-party AD auditing tools are numerous:

- **Log consolidation** – The good tools can consolidate events from large numbers of disparate DCs into a single repository (e.g., a database or file repository), which not only facilitates easier reporting and alerting, but also helps you meet any archiving requirements you might be subject to.
- **Better change detection** – In addition, some of the better auditing products don't rely on native Windows security events to detect changes to AD (or don't rely solely on them). Therefore, they can often fill in the blanks in terms of changes to AD data that Windows doesn't detect natively, or that requires extensive re-SACL'ing of your AD objects to support the required auditing.
- **Less audit data** – Third-party tools can also greatly reduce the amount of auditing data that is generated, because their custom auditing capabilities can be more efficient about how they record the data that is needed (i.e., you don't need two events to record before and after values, as native auditing requires).
- **Better auditing of GPOs** – In addition, many of the third-party products are able to detect and record specific changes to GPOs, which is something you simply can't do natively.

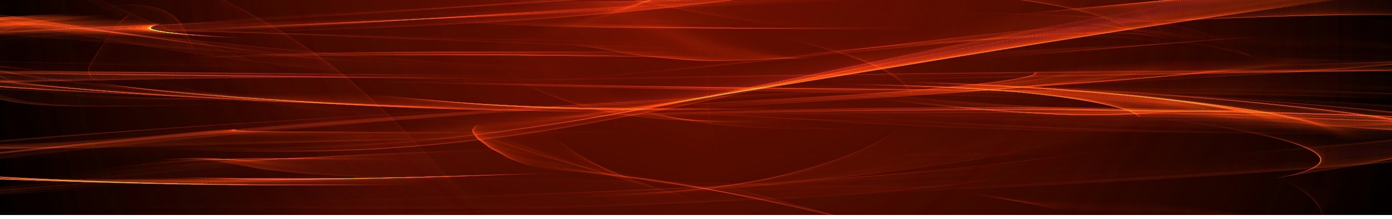
What to Look for, and What to Look Out for

Agents

If you decide to use a third-party auditing solution, you'll want to keep an eye out for a few things. First, most commercial auditing solutions need to put an agent on every one of your DCs in order to detect, alert on, and collect audit events. This is problematic for some AD shops, but it is often the only way to reliably and scalably collect audit events (and not miss anything). If you do need to install agents, just make sure the agents are certified to run on DCs—given the sensitivity of AD to most organizations, the last thing you want is an auditing product that brings your AD servers to their knees (of course, it's important to note that native auditing, if incorrectly configured, can do that by itself).

Tamper-Proof Repository

In addition, most auditors want to know that no one could have altered the content of your audit logs once the system has generated them; this is referred to as "non-repudiation." If you are using a third-party auditing product that is collecting your native Windows events (which are non-reputable



in their native state) and storing them in another repository, they (and you) need to be able to prove to an auditor that no one could have tampered with those events as they were collected and stored.

Canned Reports

You also should look for canned reports that the vendor has created for a number of different compliance or regulatory regimes. Your auditors may have different interpretations to the various regulations out there, but if the vendor has done its homework and provides canned reports in the product for the various regulatory requirements (e.g., SOX, PCI, or HIPAA), that will greatly reduce the work you have to do to make the auditors happy.

Scalability

Finally, scalability is a general concern but one that affects auditing products in particular, given the number of security events that Windows typically generates. You'll want to make sure that the third-party auditing product you choose can meet the volume of events and number of servers that your environment contains. Most vendors will have sizing guidelines for their products; you should ensure that the vendor has run in high-scale environments, if that is a requirement.

Conclusion

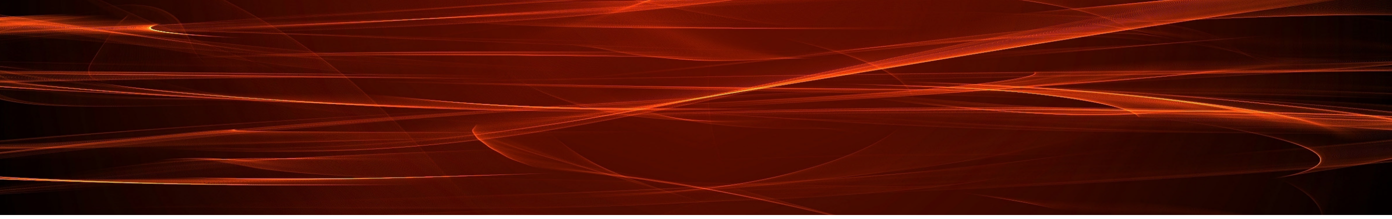
Windows natively can provide good auditing of your AD environment, especially with Server 2008 or Server 2008 R2, which include features such as before and after value auditing. But native tools have noticeable gaps in coverage (e.g., GPO changes), detail of the data, volume of data generated, centralized collecting, alerting, and reporting that can prove challenging. Auditors typically look to see that you have good controls in place around AD and its usage, and that you can readily answer questions about when key groups, users, and other objects are changed (and who made the changes).

After exploring the native functionality, you might find that third-party AD auditing solutions are the answer. Third-party solutions provide many features that Windows lacks. You need to ensure that you do your homework with respect to the coverage, reporting, scalability, and compatibility with your AD environment, but these products can go a long way toward making your auditors happy—and that makes us IT folks happy!

About the Author

Darren Mar-Elia is the CTO and founder of SDM Software. Darren has over 25 years of IT and software experience in the Microsoft technology area, including serving as a Director in Infrastructure at Charles Schwab, CTO of Windows Management Solutions at Quest Software, and Senior Director of Product Engineering at DesktopStandard, which was acquired by Microsoft.

Darren has been a Microsoft MVP in Group Policy technology for the last six years, and he has written and spoken on AD, Group Policy, and PowerShell topics around the world. Darren maintains the popular Group Policy resource site GPOGuy.com and has been a contributing editor for *Windows IT Pro* magazine since 1997. He has written and contributed to 12 books on Windows and enterprise networking topics.



Appendix: Quest Solutions for Compliance

Quest compliance solutions give you a consolidated view of your IT compliance status by assessing and providing a baseline for your environment, establishing an audit and alerting process of all events related to the security of information, and putting in place automated remediation when violations to security policies occur.

Quest compliance solutions help you address key requirements driven by internal and external regulations, and can reduce the cost and complexity of compliance within your Windows infrastructure. Tackle your most difficult compliance challenges with these Quest products:

Quest Knowledge Portal

Unified Compliance Reporting

Quest Knowledge Portal provides a unified reporting platform for a variety of Quest products. The Portal facilitates scheduled and ad-hoc reporting, enabling complete business views into IT at a summary and granular level. Authentication allows users to only view reports for which they have access. With a simple, Web-based deployment you can quickly benefit from Knowledge Portal's predefined and customizable reports and views.

Quest ChangeAuditor

Real-time Change Auditing for Your Windows Environment

Event logging and change reporting for enterprise applications and services are cumbersome, time-consuming and, in some cases, impossible using native auditing tools. Fortunately there's Quest ChangeAuditor. This product family audits, alerts and reports on all changes made to: Active Directory (ADAM/ADLDS), Exchange, EMC, NetApp, SQL Server, Windows file servers and even queries against Active Directory — all in real time and without enabling native auditing. With this award-winning tool, you can install, deploy and manage your environment from one central console. You can rely on ChangeAuditor to help you achieve your complex compliance challenges and satisfy internal security policies.

Reporter

Windows and Active Directory Reporting Tool

Quest Reporter collects, stores and reports on data from workstations, Windows servers and Active Directory, providing information essential for compliance audits, Windows security assessments or Active Directory pre- and post-migration analyses. Reporter helps administrators quickly identify trends and correlations and then rapidly resolve issues and make strategic and tactical decisions that involve the security of their Active Directory and Windows environments. Reporter decreases daily management workload by automating data collection and report generation, as a result, organizations can spend less time and money managing their infrastructure and dedicate more time to strategic improvements.

InTrust

Security Information Management & Security Event Management for Compliance

InTrust securely collects, stores, reports and alerts on event data from Windows, Unix and Linux systems, helping you comply with external regulations, internal policies and security best practices. InTrust helps you achieve regulatory compliance by auditing access to critical systems and detecting inappropriate or suspicious access-related events. With this tool, you can collect, analyze, report and generate automated real-time alerts for all relevant access-related events across your heterogeneous network. Using InTrust to monitor access to critical systems on multiple platforms reduces the complexity of event log management, saves expensive storage administration costs, improves information assurance, mitigates risk and helps to reduce cost and improve efficiency of security, operational and compliance reporting.