Realtime publishers

Protecting Critical Data by Managing the Active Directory Identity Lifecycle

Darren Mar-Elia

sponsored by

NetIQ™

Chapter 4: Auditing & Compliance and Active Directory 52
What Auditors Want 52
AD Audit Capabilities and Challenges 55
Enabling Auditing 56
Audit Categories 57
Auditing Limitations 60
Regulatory Compliance and AD 64
Compliance Best Practices and AD 67
Compliance Does Not Equal Security 68
Conclusion 68

Copyright Statement

Chapter 4: Auditing & Compliance and Active Directory

Through the previous three chapters, we've talked about the importance of managing your identities in an Active Directory (AD) world. Much of our discussion has been centered on the business and security requirements that drive identity management best practices—providing authentication and authorization to critical business applications and protecting access to vital corporate resources. But there is another benefit to having good AD identity life cycle practices: When it comes time to have to prove to auditors or regulators that you are doing all that you can to protect your systems and thus your customer's data, you have all of your t's crossed and i's dotted.

That is what this chapter is about—auditing and compliance. Many organizations, whether publicly traded or not, are subject to both internal audits and external regulatory compliance requirements. Over the years, these audit and regulations have been refined and adjusted to deal with technology advances such as AD. To that end, we now have a lot of data with which to create systems and processes that not only meet our own security and data protection requirements but also, at the same time, satisfy the auditors and regulators that we are doing what is required to protect customer and company data.

What Auditors Want

In Chapter 1, I presented the following table.

AD Auditing Punchlist			
Who made changes to a given AD object and when	Who has the ability to change AD group membership and what was changed	Who has logged into AD (and who has failed)	Which users are in AD but no longer with the company

Table 4.1: A quick list of auditing hot buttons.

These hot-button items are commonly-seen requests from auditors looking at an organization's AD environment. But from an AD perspective, there is no one clear-cut answer on what you need to have in place to satisfy every auditor. Each auditor will bring their own set of requirements to your environment, based on your business, any regulations you may be subject to, and their best practices. However, there are some broad areas that you need to ensure you have covered. The reality is that if you are managing your AD using the best practices and techniques that we've talked about in the previous three chapters, it's likely that you'll have all the information you need to satisfy auditors and regulators. Let's look at specifics of what auditors are likely going to ask of you.

To start, auditors are always interested in your ability to answer the "5 Ws"—Who, What, Where, When, Why:

- Who accessed a piece of data or made a change to a system?
- What was accessed or changed?
- Where were they when they accessed that data (that is, on the corporate network or dialed in remotely)?
- When did the access or change occur?
- Why did the access or change occur—was it appropriate or documented?

Let's talk about these five bullets in the context of managing your AD. Most if not all of these questions can be answered readily if your identity management system and AD is the central point of authentication and authorization to your systems and applications. To put it another way, if all access originates with AD or your larger identity system, you should always know who accessed a piece of data, what was accessed, where it was accessed from, when the access occurred, and why (if not directly, then through processes such as change requests or membership in a security group that grants access).

Many of the answers to these five questions, within the context of AD, can be derived from audit logs related to AD, though as we'll discuss later, auditing capabilities in a Server 2003 environment are much less encompassing than if you are running Server 2008. We'll talk about AD auditing in more detail in a bit, but first, let's look at common questions that auditors might ask in the context of your AD environment and how you might satisfy those queries within your AD life cycle management system. Table 4.2 illustrates some of these scenarios.

Auditing Scenario	Mechanisms for Satisfying the Scenario
Report group membership changes such as groups that control access to sensitive corporate data or privileged access to systems	AD audit logs can show group membership changes as well as changes to AD and related objects; server audit logs can show who has read or written to data
AD attribute changes that are sensitive (for example, password changes); disabling/enabling of user or computer accounts	AD audit logs can show changes to accounts or attributes, including who made the change and when
Ensuring that all active user accounts belong to people or applications	Usually can be handled through reporting and auditing of the provisioning and de-provisioning processes; you should be able to show, through AD audit logs, that no-longer-active employees are still logging into your systems
Creation of AD trust relationships that could affect who can authenticate to systems	AD auditing logs can show when these are created and by whom
Changes to Group Policy Objects (GPOs) that could affect security lockdown on systems	AD auditing logs show some, but can't answer the 5 Ws; you'll need third-party solutions for that. These Group Policy auditing and change management solutions deliver comprehensive audit records of all activity, answering the who, what, when, and where questions and providing before and after values for changes to GPOs, as Figure 4.1 shows.

Table 4.2: Viewing common AD-related audit scenarios.

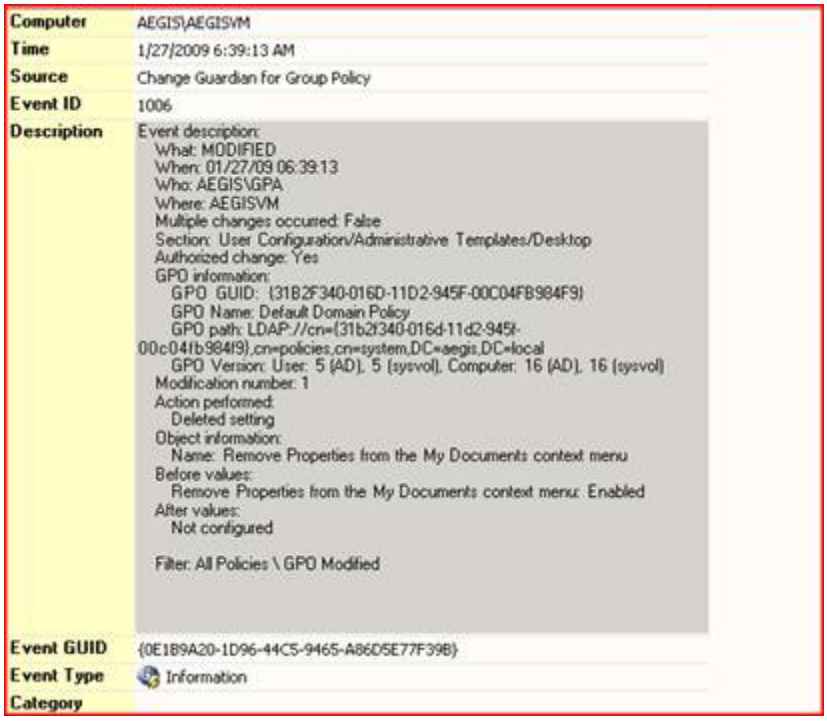


Figure 4.1: Example third-party solution providing answers to the who, what, when, and where questions for changes to GPOs.

As you can see, many of the questions that auditors will ask require that you have good auditing and reporting in place in addition to good processes, such as change management and approval-based workflows. Often times, you may need to also document these processes and workflows to prove that you have taken the time to put the processes in place and that they are used by everyone. From an auditing perspective, and especially as it relates to AD, there are practical challenges that you'll have to overcome before you can ensure that you are able to meet the requirements of the auditors. AD auditing, as it exists natively and in the box, is a complicated beast, and you'll need to learn to tame that beast before you can provide answers to the 5 Ws in a way that satisfies your auditing and compliance requirements. Let's talk about some of those challenges.

AD Audit Capabilities and Challenges

AD auditing, like the product itself, is filled with power and complexity. On the one hand, you can enable auditing at a very verbose level, such that almost any operation performed against AD can be audited. On the other hand, that verbosity can make it impractical to enable that level of auditing and there are some areas, such as Group Policy auditing, that are just lacking. Let's go through basic capabilities of AD auditing so that you can make the right call on what should be turned on within native auditing in order to be able to provide your auditors or regulators with the data they need to assess your environment's compliance to whatever regulations your organization is subject.

Enabling Auditing

Out of the box, there is *some* auditing enabled by default in AD (Server 2008 provides much more out-of-the-box auditing as well as better auditing capabilities compared with Server 2003), but it is by no means comprehensive and you're likely going to need to tweak it to meet your needs. AD auditing events are reported to the security event log on domain controllers within your AD domain. Because each "regular" domain controller is capable of both reads and writes, any AD domain controller could originate changes to AD or serve access to AD objects. As a result, there is no one security event log that you can reliably go to in order to see all changes or accesses to AD. Specifically, audit events are not replicated between domain controllers like changes to AD objects are—audit events only exist in the security event log of the domain controller that originated the change.

You will need to have a system in place that collects (and alerts on, if required) audit events from all domain controllers. In addition, you need to be cognizant of the volume of auditing that you enable. Windows Server 2008 and newer provides more granular ability to turn on and off categories of auditing. However, it's not uncommon, in large AD environments, that during normal activity, a security event log of 50MB could roll over quite rapidly. In other words, the events happening against AD cause the 50MB to be taken up and the log starts writing new events by deleting old ones. I've seen environments where the security log on a given domain controller will roll over in a matter of 20 to 30 minutes! That means that you need to be capturing and archiving events across all those domain controllers **as they are happening**, otherwise, they are lost forever and not available to your auditors, regulators, or your own security team.

Enabling auditing of AD events can be a two-part process, depending upon what you need to audit. As I mentioned, there is the enabling of AD auditing "categories" to tell Windows which types of events to audit on. In addition, if you need to audit changes to AD objects—for example, you want to know when the department attribute on a set of users has changed—then in addition to enabling the category for AD changes, you need to set a System Access Control List (SACL) on that object's security permissions in AD. For example, if you want to audit changes to that department attribute on all users within the "Marketing OU" of your domain, you can use the AD Users and Computers MMC snap-in to modify the security on that OU and apply the SACL, as Figure 4.2 shows.

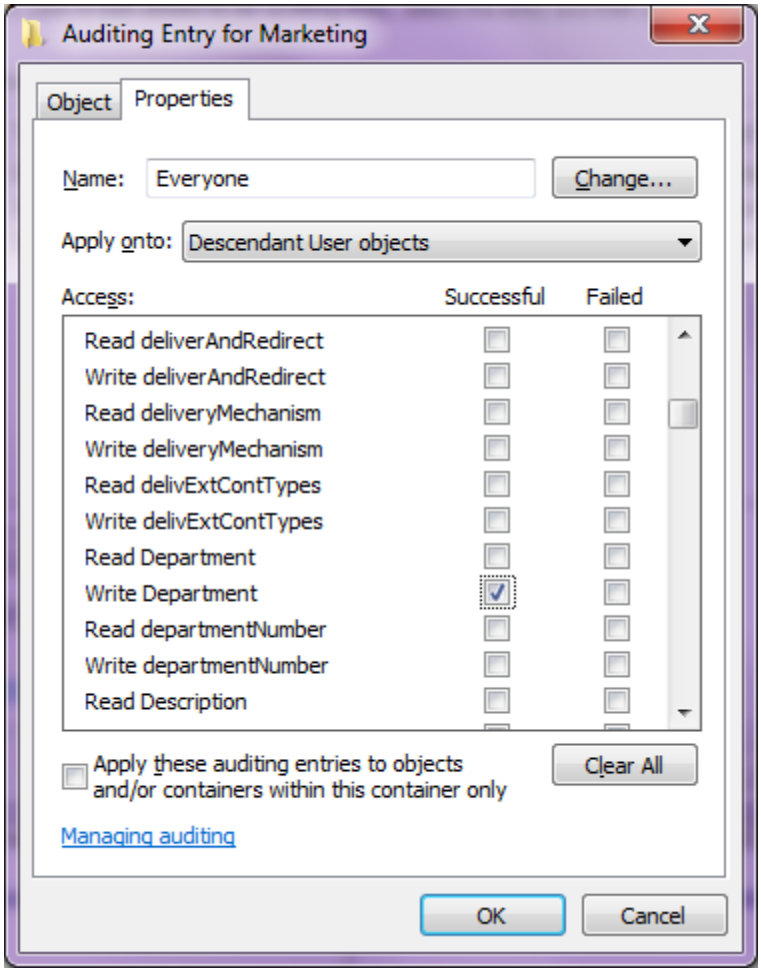


Figure 4.2: Setting an SACL on the Marketing OU.

As Figure 4.2 shows, you are telling Windows that for the group "Everyone," which means all users in AD, audit any writes to the department attribute for user objects within the Marketing OU. Without this SACL in place, even if you have the category for AD auditing enabled, you should not see these department attribute writes in the security event log of the domain controller originating the change.

Audit Categories

We've talked briefly about audit categories as the other piece of the puzzle for enabling auditing within AD. These categories come in two flavors, depending upon the version of Windows you're running. For Server 2003 environments, there is what I'll call the "legacy" auditing categories:

- Audit Account Logon Events
- Audit Account Management
- Audit Directory Service Access
- Audit Logon Events

- Audit Object Access
- Audit Policy Change
- Audit Privilege Use
- Audit Process Tracking
- Audit System Events

These audit categories are fairly broad. From an AD perspective, the most interesting ones are the "Account Logon Events," "Account Management," and "Directory Service Access" categories. These categories, when enabled, allow you to audit logons and logoffs to AD, changes to user and group accounts, and access to and changes to AD itself, respectively. Note that for the first two categories listed, you don't need to set SACLs on AD objects. Once those two categories are enabled, AD logons and logoffs as well as change events related to groups, user, and computer accounts will be audited. That may be a bit confusing because these are AD objects, and you would assume that you would need to enable Directory Service Access auditing in order to see these changes. However, that is not the case, at least for users, groups, and computer accounts.

You can configure these basic audit categories through Group Policy, as Figure 4.3 shows.

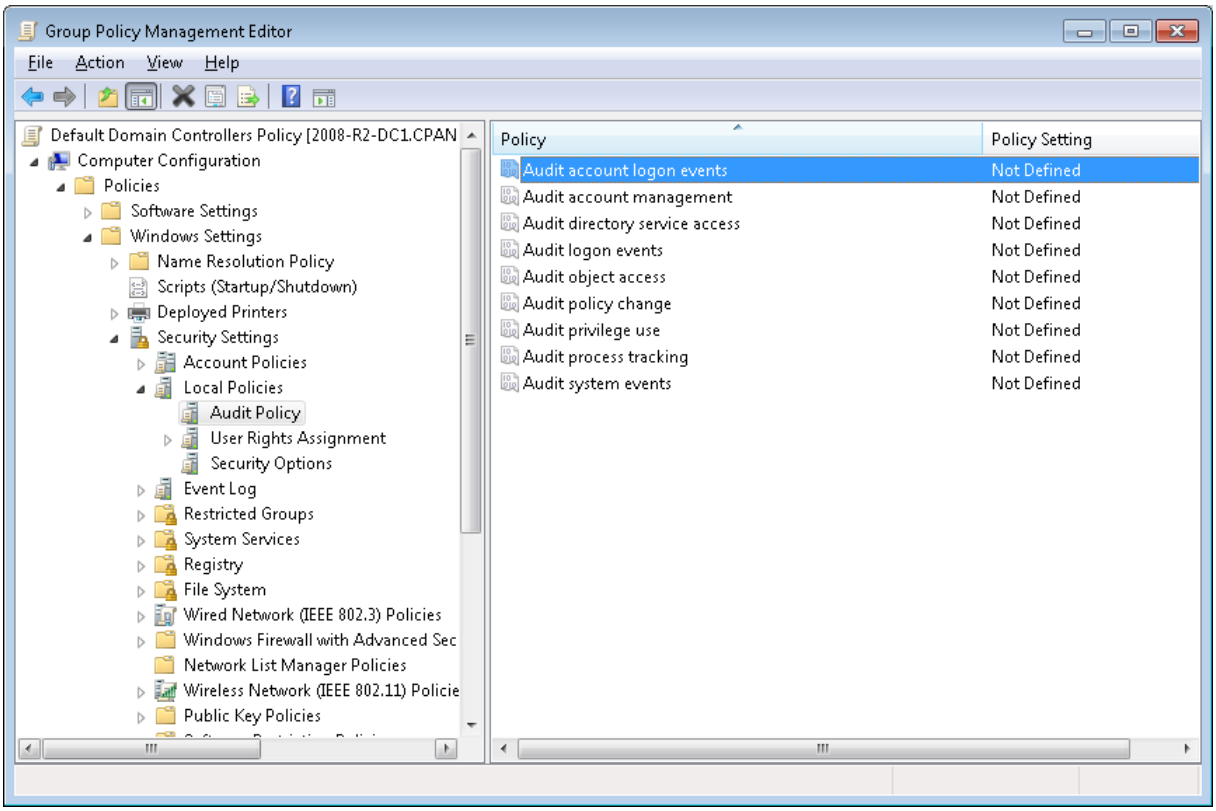


Figure 4.3: Configuring basic audit categories through Group Policy.

When these audit category policies are applied to a GPO that is processed by your AD domain controllers (for example, the Default Domain Controllers Policy), they will affect the auditing of AD-based events, which is what you want.

In addition to these basic categories, and perhaps in recognition of the verbosity of auditing events that are generated when one or more of these categories is enabled, Microsoft provided the capability of enabling more granular auditing when the company introduced "Advanced Audit Configuration" starting with Server 2008. This new capability was first exposed via a command-line utility called **auditpol.exe**, which you could use to enable more granular auditing. When Server 2008-R2 shipped, Microsoft exposed the management of these granular audit sub-categories through Group Policy (see Figure 4.4).

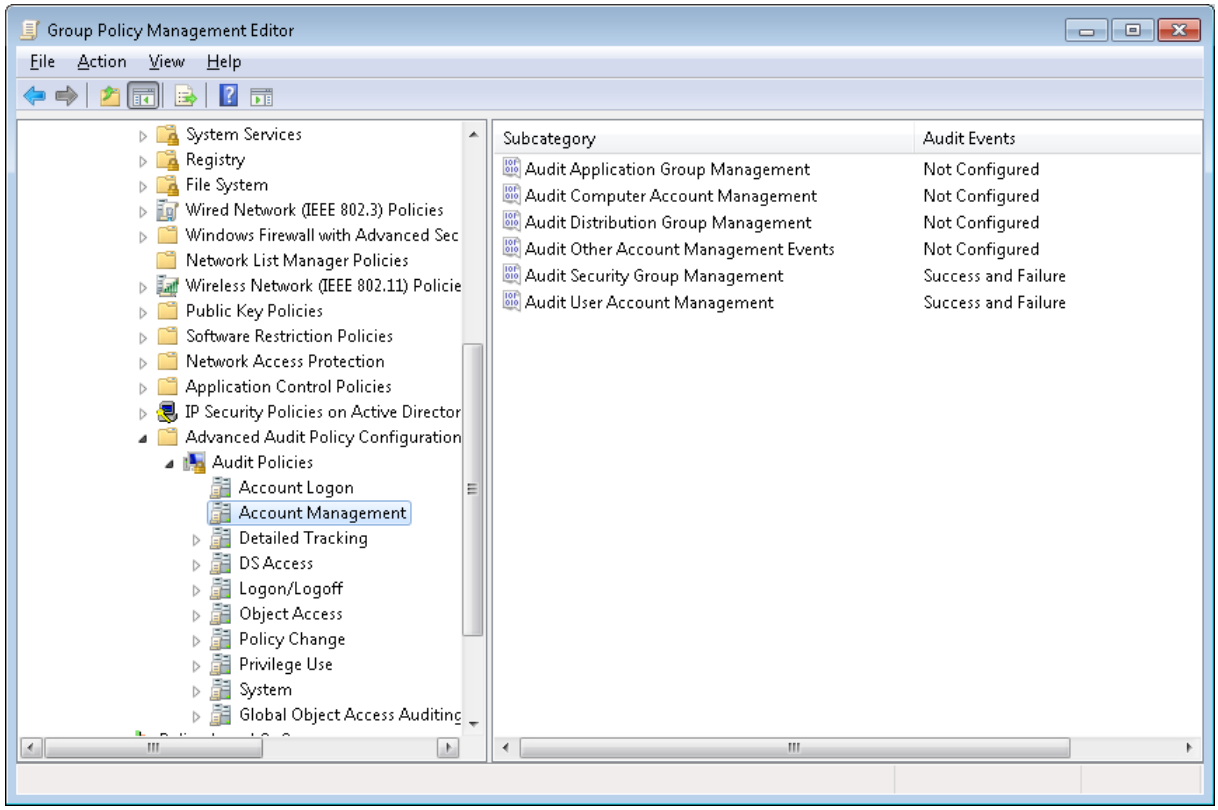


Figure 4.4: Viewing the detailed audit sub-categories in Server 2008-R2.

What you'll notice about these sub-categories is that they start with the general "legacy" categories and add the ability to enable or disable more granular auditing within each of the larger categories. This allows you to enable only the auditing that you need to meet your security, auditing, and compliance requirements and reduces the chance of log rollover. Of course, all of your AD domain controllers will need to be running at least Server 2008 to support these new sub-categories.

Working with the New Audit Sub-Categories

If you've been working with the older general audit categories and are planning to shift towards using the new sub-categories, there's one setting you'll need to enable within Group Policy for all your AD servers that will be using the new audit sub-categories. Specifically, you'll need to enable the setting called **Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Audit: Force audit policy subcategory settings (Windows Vista or later)**. Without this setting enabled, Windows will ignore the more granular settings and only pay attention to the "legacy" categories.

Auditing Limitations

Once auditing is enabled in your AD environment, you will start generating lots of audit events within your AD domain controller security logs. And of course, you'll need to start collecting and archiving these in order to be able to show them to auditors and your own security staff. Unfortunately, there are holes within native AD auditing that you'll have to be cognizant of as you dive into the process of fully auditing your environment. Although AD auditing is pretty good and continues to get better with every new Windows release (audit coverage in Server 2008-R2 is quite a bit better than Server 2003), there are still gaps. Let's highlight the biggest areas to be concerned about as you are moving to get full audit coverage for your AD environment.

Limitation	Challenges
Before and after values for AD object changes are only logged starting in Server 2008	The downside here is that these are logged as two separate events in the security logs of the originating domain controller; thus, you have to correlate the two events whenever a change occurs
Some audit data is not presented in a human-readable way	For example, changes to AD object security descriptors appear as long Security Descriptor Definition Language (SDDL) strings that are not human readable without formatting
AD changes are only audited on the originating domain controller	This means that you will have to consolidate log events across all domain controllers in order to have a total view of all events happening within AD

Audit logs can roll over quickly on large, busy systems; no means of natively archiving	This means that you'll need some way of collecting and alerting on events in near-real-time in order to not lose events within your environment
GPO changes are not audited in any detail	Native auditing does not provide any details about what settings were changed within a GPO; if DS Access auditing is enabled, you will see at least who made a GPO change but not what the change was

Table 4.3: Viewing limitations within the native auditing infrastructure.

Table 4.3 underscores challenges of meeting your auditing needs with native capabilities. The good news is that there are several third-party vendors on the market that have products that plug one or more of these holes in order to give you a complete auditing system. For example, a third-party solution (see Figure 4.5) can address the challenge of native event logs providing information in a non-human-readable format (for example, those SDDL strings) by presenting the audit data in a translated, usable format for the administrator or auditor.

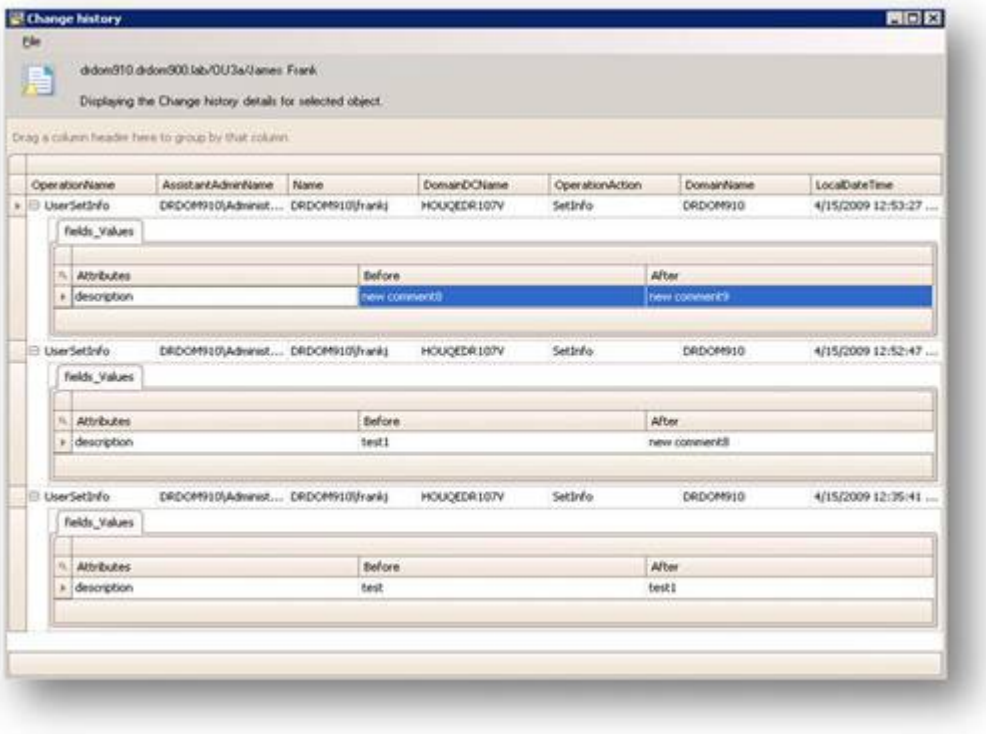
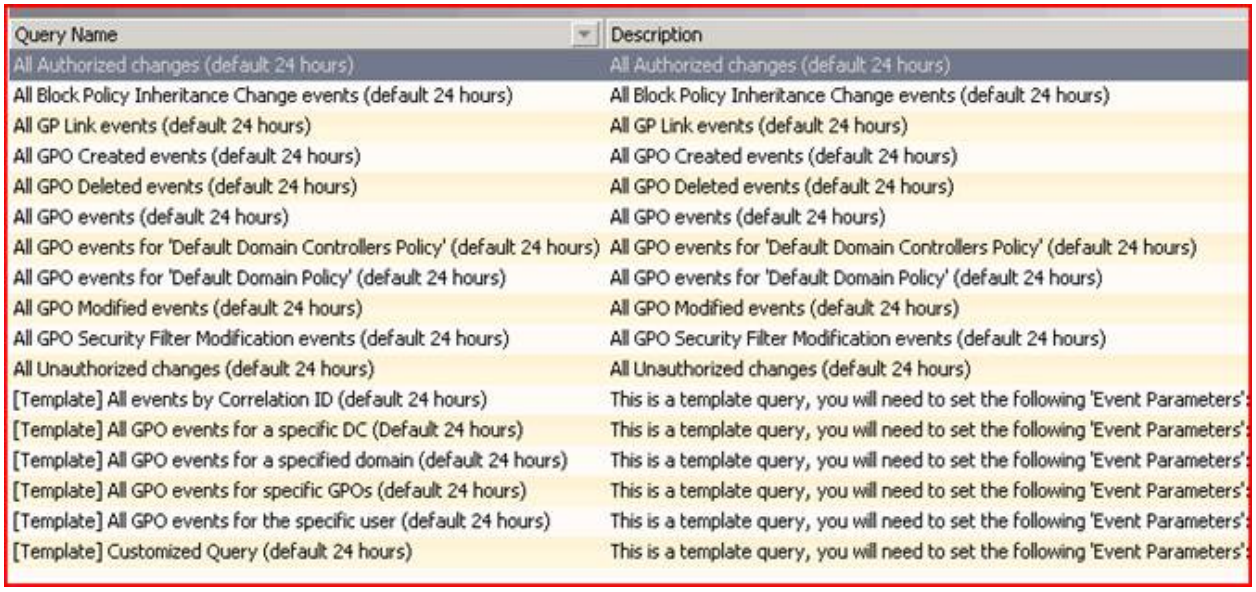


Figure 4.5: An example third-party solution presenting audit data in a translated, usable format for the administrator or auditor.

Additionally, as seen in Figure 4.6, third-party Group Policy auditing and change management solutions can provide proactive monitoring and meaningful reporting of changes to GPOs that could affect security lockdown on systems.



Query Name	Description
All Authorized changes (default 24 hours)	All Authorized changes (default 24 hours)
All Block Policy Inheritance Change events (default 24 hours)	All Block Policy Inheritance Change events (default 24 hours)
All GP Link events (default 24 hours)	All GP Link events (default 24 hours)
All GPO Created events (default 24 hours)	All GPO Created events (default 24 hours)
All GPO Deleted events (default 24 hours)	All GPO Deleted events (default 24 hours)
All GPO events (default 24 hours)	All GPO events (default 24 hours)
All GPO events for 'Default Domain Controllers Policy' (default 24 hours)	All GPO events for 'Default Domain Controllers Policy' (default 24 hours)
All GPO events for 'Default Domain Policy' (default 24 hours)	All GPO events for 'Default Domain Policy' (default 24 hours)
All GPO Modified events (default 24 hours)	All GPO Modified events (default 24 hours)
All GPO Security Filter Modification events (default 24 hours)	All GPO Security Filter Modification events (default 24 hours)
All Unauthorized changes (default 24 hours)	All Unauthorized changes (default 24 hours)
[Template] All events by Correlation ID (default 24 hours)	This is a template query, you will need to set the following 'Event Parameters'
[Template] All GPO events for a specific DC (Default 24 hours)	This is a template query, you will need to set the following 'Event Parameters'
[Template] All GPO events for a specified domain (default 24 hours)	This is a template query, you will need to set the following 'Event Parameters'
[Template] All GPO events for specific GPOs (default 24 hours)	This is a template query, you will need to set the following 'Event Parameters'
[Template] All GPO events for the specific user (default 24 hours)	This is a template query, you will need to set the following 'Event Parameters'
[Template] Customized Query (default 24 hours)	This is a template query, you will need to set the following 'Event Parameters'

Figure 4.6: An example third-party Group Policy auditing and change management solution offering proactive monitoring and meaningful reporting of changes to GPOs.

In order to bring all these pieces together, let's walk through a common auditing scenario that you might need to report on to your auditors: tracking changes to security group membership. There are at least a couple of ways you can track such a change. You could enable the Account Management audit category. This in and of itself would give you what you needed in terms of tracking group membership changes (see Figure 4.7).

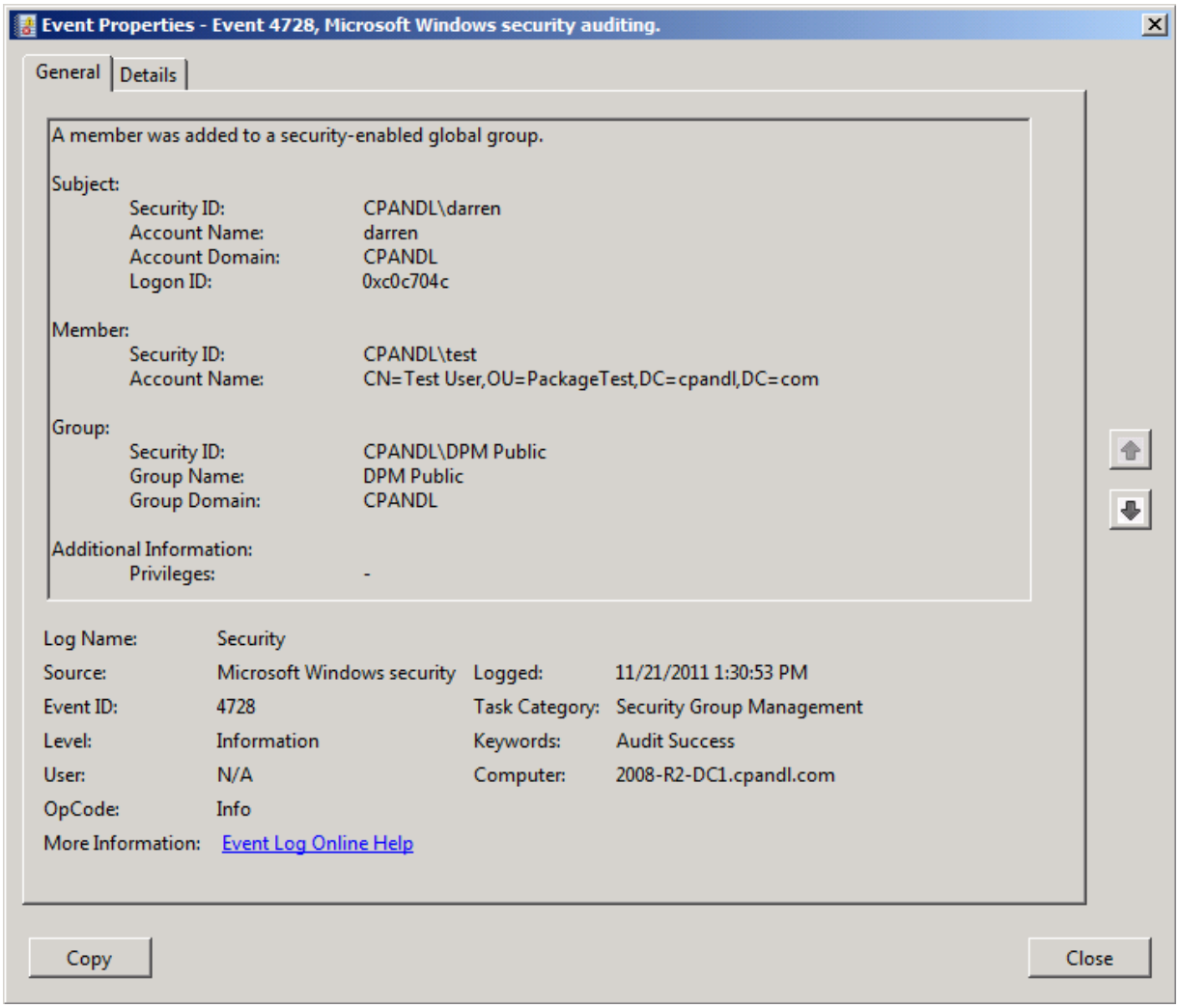


Figure 4.7: Viewing a group membership change as tracked by Account Management auditing.

The alternative is that you could enable DS Access auditing and then set an SACL on the group that you're looking to monitor. The SACL would look for writes to the "Members" attribute. This latter approach is obviously more cumbersome because you would have to set SACLs on the objects you want to audit in addition to enabling DS Access auditing, but the results, as you can see in Figure 4.8, are roughly the same.

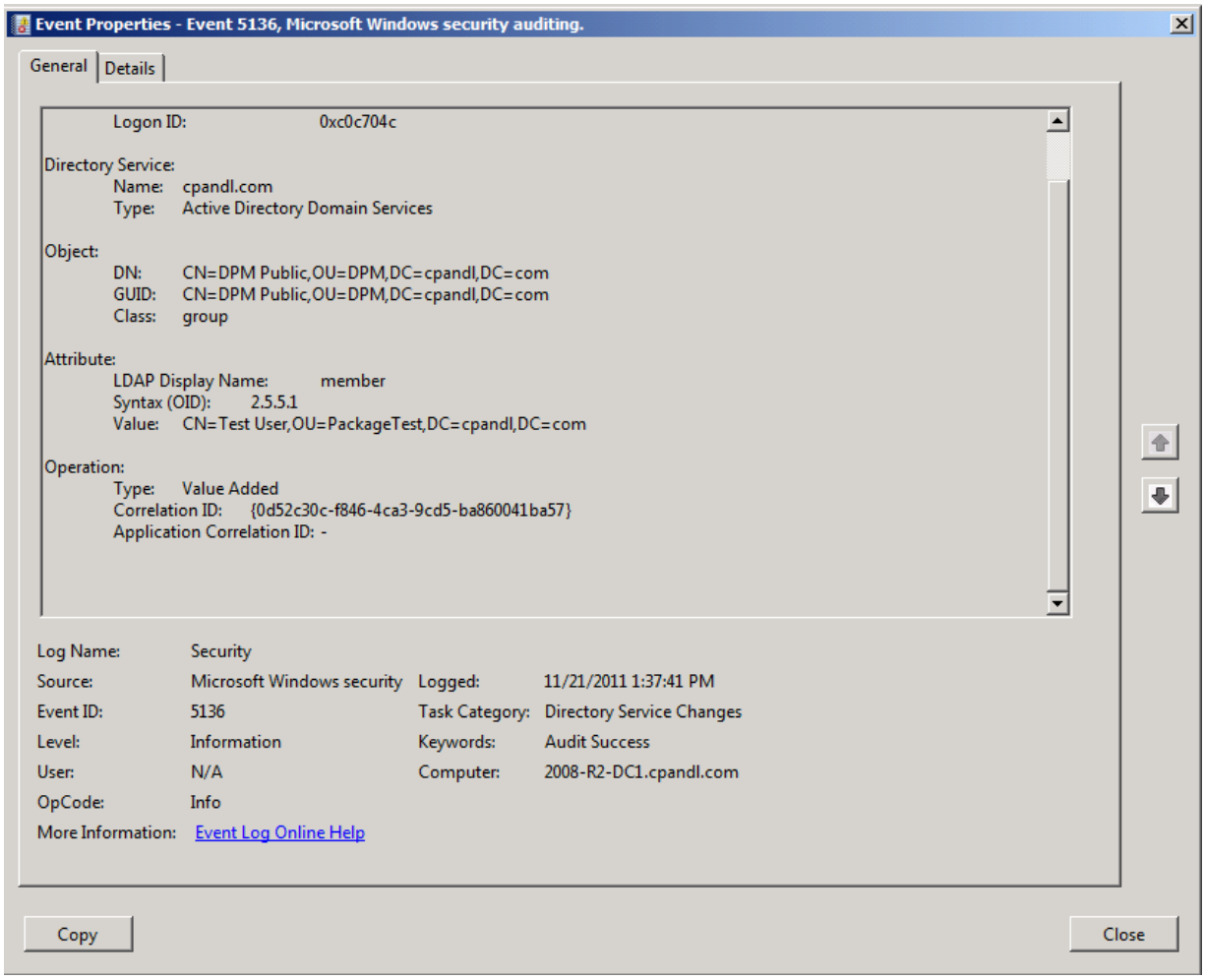


Figure 4.8: Auditing group membership changes via SACLs.

With an established foundation on the capabilities and limitations of AD auditing, let's shift gears and talk about regulatory compliance as it relates to AD.

Regulatory Compliance and AD

In the past 10 or so years, a number of government regulations have come about that have a direct impact on how you run your Identity Management systems, and thus how you run AD. Some of these regulations include:

- The Sarbanes-Oxley ACT, which is related to financial reporting of public companies
- The Health Insurance Portability and Accountability Act (HIPAA), which is related to the control and release of health care data associated with patients
- Payment Card Industry (PCI) regulations, which are related to credit card reporting and recordkeeping.
- The Gramm-Leach-Bliley Act, which is related to control and release of customer information

Although there are not precise descriptions within the text of these regulations that says, "Thou shall configure your AD in the following way to be compliant," as time has passed, regulators, auditors, lawyers, and compliance officers within organizations have gotten past the vague language of the regulations and started to drill into what they mean to the various practical aspects of running IT, and especially of how identity management (and by definition, AD) plays a role.

The bottom line for many of these regulations is about control—control of data, control of access, and knowing at all times who is accessing what data. This kind of control is what we've been talking about for four chapters, related to proper AD and identity management, so you can imagine that there is an important role to play for AD in the management, auditing and reporting of such controls. How does that impact AD? Well, as we've talked about, AD is often the central point of control for many organizations, in terms of authentication and authorization to systems, applications, and data. You can imagine that some of those applications are related health care patient records and some of that data is customer Social Security Numbers or other private information. When you think of it this way, AD then takes on a very crucial role in terms of protecting those applications and data, and ensuring that the right people have access to that information. And, in brass tacks terms, this means that the right users are in the right security groups that grant them proper access to these sensitive areas of the organization.

Let's look in detail how one regulation in particular, the PCI Data Security Standard (PCI DSS), and its requirements can directly impact how you manage your identity systems in general and AD in particular. PCI DSS 2.0, for example, has a number of requirements that companies that handle credit card data must adhere to, including:

- Develop configuration standards for all system components
- Restrict access to cardholder data by business need-to-know
- Ensure proper user authentication and password management for non-consumer users and administrators on all system components
- Secure audit trails so that they cannot be altered
- Maintain a policy that addresses information security for employees and contractors

Each of these bullets speaks directly to an aspect of identity management and/or AD. Table 4.4 talks to how you can use AD (or controls related to it) to address each of these issues.

PCI Requirement	How AD Can Help
Develop configuration standards for all system components	Group Policy is often used to secure and configure Windows systems. As such, management and auditing of Group Policy changes becomes critical so that you know when Group Policy changes could cause systems to deviate from standards. In addition, because Group Policy itself can grant access to systems, its use must be tightly controlled to meet this requirement.
Restrict access to cardholder data by business need-to-know	Cardholder data is likely held on systems that require authentication and authorization to access them. And that access is often tied to an organization's identity system, including AD. In that case, tight control over the ability to provision who is placed in groups that allow access to that cardholder data is important, as is the ability to audit and report on use of that access through AD and server auditing.
Ensure proper user authentication and password management for non-consumer users and administrators on all system components	This requirement speaks to both the management of the provisioning process to ensure that users and administrators are placed in the correct AD security groups for their job role and auditing the use of these groups for accessing systems, especially within an administrative capacity.
Secure audit trails so that they cannot be altered	This speaks to the topic of non-repudiation of event logs that came up in Chapter 2. AD and its security logs provide this protection out of the box, but the moment you use a third-party product to consolidate events elsewhere (for example, in a database), you need to ensure that such non-repudiation is maintained—especially if you plan to use that external data store for auditing and compliance reporting.
Maintain a policy that addresses information security for employees and contractors	This speaks to more of a process around ensuring that all users of your systems are aware of the policies for securing PCI-related information. However, the process can be backed up within your AD by appropriate provisioning of users and groups and by complete auditing of user access to systems, applications, and data.

Table 4.4: Viewing an example of how AD and related processes can address PCI-DSS compliance.

Compliance Best Practices and AD

Meeting your compliance requirements goes hand in hand with all the aspects of good AD management that we've talked about thus far. Having tight control over the user provisioning and de-provisioning process; maintaining good change processes for things like Group Policy changes, AD configuration changes, and group membership changes; and ensuring good auditing and reporting are in place will go a long way towards satisfying auditors and compliance officers' needs . Let's re-cap some of these best practices in the context of compliance with regulations:

- Ensure that you have a good provisioning and de-provisioning process in place that grants least-privilege access to systems and resources (and removes it when the user's role changes or they leave the organization)
- Ensure that you have periodic attestation for things like security group memberships with group owners checking that users still belong in the groups they are members of
- Ensure that Group Policy changes go through a change control process and are audited periodically for unscheduled changes. Again here, third-party vendors can provide Group Policy auditing and change management solutions to fill the gaps in the native solutions provided by Microsoft and help provide a secure and auditable environment.
- Ensure that auditing is enabled to track changes to and use of AD and that audit logs are archived and alerted on for critical events
- Have ready access to audit events that track changes or access, especially when critical or sensitive systems or resources are involved

These bullets really represent a roll-up of all the points I've made throughout this book. Simply said, if you are doing good identity management and AD management, you should have no problem with your compliance and auditing requirements. That being said, it's also important to remember that compliance to regulations and auditors is a "side benefit" of managing your identity systems well. The real benefit is a secure environment that protects critical organizational data and systems.

Compliance Does Not Equal Security

Throughout this book, we've talked about the important role that your identity systems and especially AD play in controlling access to critical resources. All of the best practices that we've discussed so far are around protecting that data that is the lifeblood of your organization. It's important to keep in mind that, while regulatory compliance is often critical for your company to do business, it is means to an end rather than an end in and of itself. That is, the end goal is to protect your company's data and systems so that your company can do its job. The fact that a regulatory body is checking up on you to ensure that you are actually doing that work is important, but secondary. No regulatory compliance will help if you expose critical data because some piece of your identity system was left unmanaged because regulators did not require you to manage it. If you are doing all that you can to protect your company's systems and data, the regulatory compliance will often follow, or if it does not straight away, then you will have the tools to meet your compliance goals without a major re-work of your identity system. Put simply, take care of your identity systems and how they're used and the rest will follow!

Conclusion

Throughout this book, we've talked about the importance of getting control of your identity management systems, and by extension, one of the most important players in that system—AD. You must implement control for every aspect, whether creating a life cycle for identity provisioning and de-provisioning—from creating to updating to auditing and removing identities to securing AD. And there are a set of steps that you must undertake to ensure that you have control over access to critical business resources. And, when it comes time to audit the use of AD, you must choose between taking advantage of the tools that are "in the box" or looking to third-parties to help fill the gaps. Regardless, if you build your AD-based identity system on the principles we've discussed, when auditors and compliance officers come knocking, you'll be prepared to provide the reports and data necessary to show that you are doing your job in protecting your organization's most precious commodity—its data.