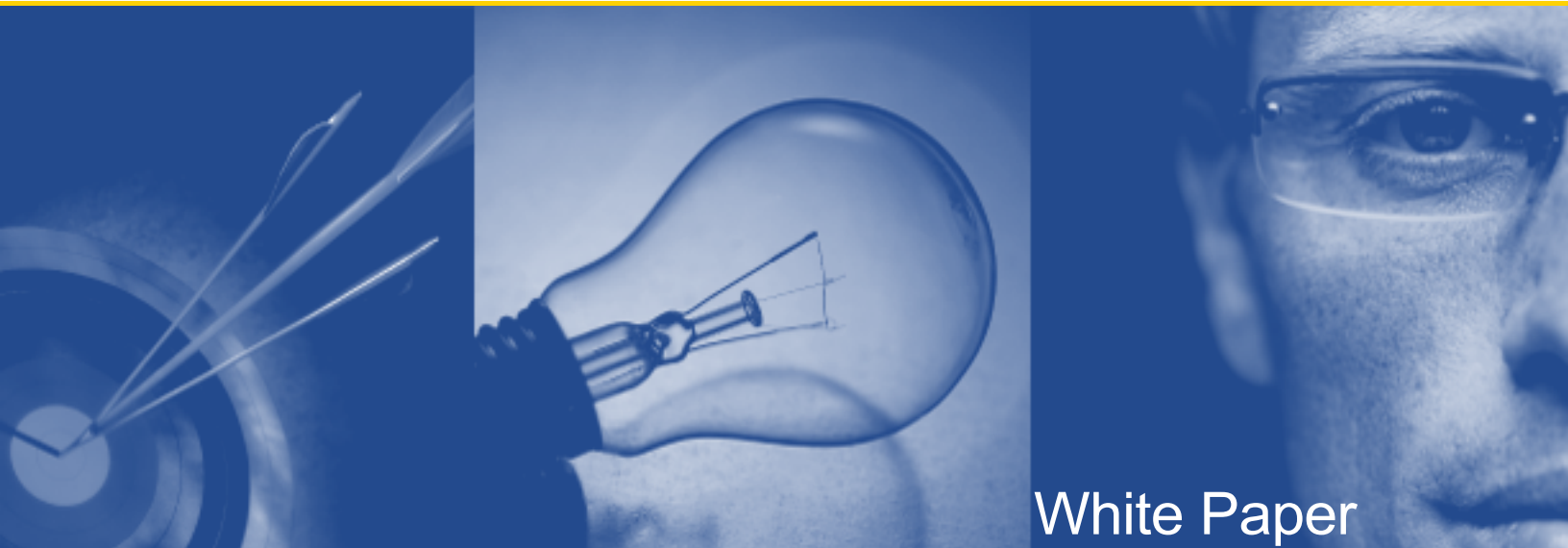


Overcoming Active Directory Audit Log Limitations

*Written by
Randy Franklin Smith
President
Monterey Technology Group, Inc.*



White Paper

**© 2009 Quest Software, Inc.
ALL RIGHTS RESERVED.**

This document contains proprietary information, protected by copyright. No part of this document may be reproduced or transmitted for any purpose other than the reader's personal use without the written permission of Quest Software, Inc.

WARRANTY

The information contained in this document is subject to change without notice. Quest Software makes no warranty of any kind with respect to this information. QUEST SOFTWARE SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTY OF THE MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Quest Software shall not be liable for any direct, indirect, incidental, consequential, or other damage alleged in connection with the furnishing or use of this information.

TRADEMARKS

All trademarks and registered trademarks used in this guide are property of their respective owners.

World Headquarters
5 Polaris Way
Aliso Viejo, CA 92656
www.quest.com
e-mail: info@quest.com

Please refer to our Web site (www.quest.com) for regional and international office information.

Updated—October 2009

CONTENTS

- EXECUTIVE SUMMARY 1**
- INTRODUCTION 2**
- KEY REGULATORY PROVISIONS FOR MONITORING ACTIVE DIRECTORY 3**
 - THE SARBANES-OXLEY ACT OF 2002 (SOX) 3
 - PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI) 4
 - THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002 (FISMA) 4
- HOW FAR DOES THE NATIVE AUDIT LOG TAKE YOU? 5**
 - ACCOUNT MANAGEMENT 5
 - DIRECTORY SERVICE ACCESS 6
 - IMPORTANT GAPS AND LIMITATIONS 6
 - No Centralized Audit Trail* 6
 - No Reporting or Analysis* 6
 - High Volume of Audit Data* 6
 - Performance Risks* 7
 - Missing or Limited Information* 7
 - Lack of Real-time Monitoring and Alerting* 7
 - No Protection from Privileged Administrators* 7
- BRIDGING THE GAP: QUEST CHANGEAUDITOR FOR ACTIVE DIRECTORY 8**
- CONCLUSION 10**
- ABOUT THE AUTHOR 11**
- ABOUT QUEST SOFTWARE, INC. 12**
 - CONTACTING QUEST SOFTWARE 12
 - CONTACTING QUEST SUPPORT 12
- NOTES 13**

EXECUTIVE SUMMARY

Much of the security and control of an enterprise IT environment rests on Active Directory. It provides authentication and access control for Windows users and applications, as well as for UNIX, Linux and mainframes. Even VPNs, extranets and internal network security technologies all use Active Directory for policy and identity information.

To comply with information security best practices and compliance requirements, Active Directory must be regularly monitored and audited. However, the native Windows security log provides only limited Active Directory audit capabilities, preventing organizations from achieving full compliance with best practices and security requirements.

Quest ChangeAuditor for Active Directory bridges the gaps in the native security log by enabling organizations to efficiently monitor high-impact and suspicious modifications to Active Directory, as well as comply with regulatory and industry requirements.

INTRODUCTION

Active Directory is the cornerstone of security and control in today's corporate network. Active Directory accounts are the first point of authentication and access control when users log on to their workstations. Also, many applications integrate with Active Directory and use those accounts to authenticate and control access to their hosted information and transactions. Active Directory groups are used throughout the Microsoft environment to control access to resources; applications use them to control entitlements and authorization.

Beyond identity services, Active Directory also hosts security configuration policies for the many Windows computers within an enterprise network. Thanks to the wide support of LDAP and Kerberos, Active Directory also provides authentication and directory services to other operating systems and platforms, including UNIX, Linux and mainframes. Active Directory also provides the automation and policy storage required by public key infrastructures based on Windows Certificate Services. VPNs, extranets and internal network security technologies such as Network Access Protection and Network Access Control all depend on Active Directory for policy and identity information.

Because nearly every component of the enterprise IT environment relies on Active Directory, the importance of the security and health of Active Directory cannot be overstated. In addition, to comply with regulatory requirements, organizations must monitor and quickly respond to high-impact or suspicious changes in Active Directory and produce audit trails documenting that key controls and security processes were followed.

This white paper outlines key provisions of several regulations that affect many organizations, explains how the native audit log can help organizations achieve compliance and discusses the log's limitations. It then explains how Quest ChangeAuditor for Active Directory can address those limitations and bring organizations into full regulatory compliance.

KEY REGULATORY PROVISIONS FOR MONITORING ACTIVE DIRECTORY

This brief overview describes key provisions in several regulations that illustrate why it is critical to monitor and audit Active Directory. While compliance regulations may differ in scope and the types of protected information, they all share common requirements. Protecting any type of information involves common best practices.

The Sarbanes-Oxley Act of 2002 (SOX)

SOX applies to most publicly traded companies and seeks “to protect investors by improving the accuracy and reliability of corporate disclosures.” To reach this goal, SOX makes corporate executives and public accounting firms liable for the quality of financial reports and other disclosures to investors. But SOX goes further; it mandates that certain “best-practice” activities are now law and requires directors of publicly held companies to report on their performance of these activities. Companies are required to select and use a control framework to evaluate the effectiveness of the company’s internal financial reporting controls. COBIT¹ is the most commonly used framework.

Monitoring is a prominent component of COBIT; in fact, “Monitor and evaluate” is one of its “Four Interrelated Domains.” Monitoring and auditability requirements are specified by multiple controls defined in COBIT, including

- DS5 Ensure Systems Security
 - DS5.3 Identity Management

Active Directory is the core technology used by organizations for identity management. COBIT requires organizations to “confirm that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by system owners and implemented by the security-responsible person.”
 - DS5.4 User Account Management
 - DS5.5 Security Testing, Surveillance, and Monitoring
- DS9 Manage the Configuration
 - DS9.2 Identification and Maintenance of Configuration Items

“Record new, modified and deleted configuration items”
 - DS9.3 Configuration Integrity Review

“Review and verify on a regular basis, using, where necessary, appropriate tools, the status of configuration items...”

Payment Card Industry Data Security Standard (PCI)

Developed by an alliance of credit card companies to protect payment account data, PCI mandates very specific monitoring and availability controls. Requirement 10 of PCI's 12 requirements is "Track and monitor all access to network resources and cardholder data." At many organizations, Active Directory is a key component of the cardholder data network (CDN) defined by PCI.

The Federal Information Security Management Act of 2002 (FISMA)

FISMA requires all federal agencies to improve the security of federal information and information systems. FISMA also affects many commercial companies, because the requirements apply equally to federal systems as well as information maintained by government contractors. The National Institute of Standards and Technology developed NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems," as a technical guide to implementing FISMA controls.

NIST SP 800-53 defines the controls for monitoring and auditability in any organization using Active Directory. For example, the Audit and Accountability section includes nine different controls that must be applied to any core technology component such as Active Directory:

- AU-1 - Audit and Accountability Policy and Procedures
- AU-2 - Auditable Events
- AU-3 - Content of Audit Records
- AU-4 - Audit Storage Capacity
- AU-5 - Audit Processing
- AU-6 - Audit Monitoring, Analysis, and Reporting
- AU-7 - Audit Reduction and Report Generation
- AU-8 - Time Stamps
- AU-9 - Protection of Audit Information

Other notable controls in NIST SP 800-53 include:

- CA-7 Continuous Monitoring
- CM-4 Monitoring Configuration Changes
- IR-5 Incident Monitoring

To summarize, compliance regulations are simply best practices in legislative or contractual form. Although this section does not cover every regulation, it is safe to assume that proper Active Directory monitoring and auditability is required to achieve compliance with many internal and external requirements.

HOW FAR DOES THE NATIVE AUDIT LOG TAKE YOU?

Because Active Directory monitoring and auditability is so important, Windows Server provides some native functionality for auditing changes and other high-priority Active Directory events. This section provides an overview of the native Active Directory audit features of the Windows security log and identifies their limitations.

Windows Server provides Active Directory audit capabilities through two Windows security log categories: Account Management and Directory Service Access. The Directory Service category provides low-level auditability of every object and attribute in Active Directory, while the Account Management category provides higher level auditing of users, groups and computers.

Account Management

The Account Management category of the Windows security log allows you to monitor the creation, modification and deletion of users, groups and computer objects in Active Directory. You can use Account Management events to track things such as new user accounts, password resets, and new group members. Monitoring the maintenance of domain users and groups can be a key aspect of compliance with legislation such as SOX and Health Insurance Portability and Accountability Act (HIPAA); access to private or financially significant information is largely controlled through group membership and based on user-account authentication.

When you enable this category on DCs, each DC begins recording maintenance events that are executed against its users, group, and computer objects. To get a complete record of all Account Management events for AD objects, you'll need to combine this category's activity from all your DC Security logs. The table below shows the subcategories that are associated with Account Management.

ACCOUNT MANAGEMENT SUBCATEGORY	TRACKS CHANGES TO
User Account Management	Server local user and AD user accounts
Computer Account Management	AD computer accounts
Security Group Management	AD security groups and local server groups
Distribution Group Management	Mail accounts for Exchange
Application Group Management	Role-based authorization groups for applications
Other Account Management Events	Policy change events

Account Management audits changes to users, groups, and computers, but does not provide any auditing for other critical changes to Active Directory, such as modifications to Group Policy Objects (GPOs), organizational units (OUs), delegated administrative authority, trust relationships or other policies.

Directory Service Access

A misstep in AD can adversely affect thousands of users or computers within minutes, so being able to determine who changed what in AD is critical. While Account Management events provide user, group and computer maintenance auditing, Directory Service Access events make low-level auditing available for all types of AD objects. Directory Service Access events identify the object that was accessed and by whom, and also document the accessed object properties.

Important Gaps and Limitations

Despite the valuable functionality provided by the Windows security log, significant gaps and limitations remain. These compromise an organization's ability to fulfill security and regulatory requirements for monitoring and auditing Active Directory.

No Centralized Audit Trail

At most organizations, Active Directory includes multiple domains; fault tolerance, scalability and bandwidth requirements are fulfilled by the deployment of multiple domain controllers for each domain. While directory information is replicated between domain controllers, security logs are not; each domain controller has its own security log, which contains only the events associated with operations performed against that particular domain controller. Therefore, an organization's overall audit trail is fragmented across many domain controllers within the Active Directory environment.

Most versions of Windows Server lack any mechanism for collection of security logs into a central repository. While the new event forwarding feature of Window Server 2008 may be of interest for smaller networks, it does not adequately address this important gap for larger enterprises because of scalability and maintenance limitations.

No Reporting or Analysis

Windows Server provides no real reporting or analysis capabilities for the Windows security log. The only native tool for viewing security log activity is the Event Viewer Microsoft Management Console, which provides only basic filtering capabilities. Administrators and auditors lack any way to massage the raw security log data into informative and actionable reports.

High Volume of Audit Data

Because of the low-level, generalized nature of the Directory Service Access category, the Windows security log can produce huge amounts of data when used to audit Active Directory changes. With each domain controller producing potentially hundreds of megabytes of audit data every day, locating critical events is like looking for a needle in a haystack—and vast storage is required to archive the audit data.

Performance Risks

Given the huge amounts of audit data and the arcane nature of policy definition, it is easy to define Active Directory audit policies that quickly overwhelm any amount of domain controller hardware.

Missing or Limited Information

While Active Directory does a good job of reporting that an object was modified, the security log often fails to explain what was changed about the object. For instance, only domains hosted by Windows Server 2008 domain controllers provide the actual data values of attribute changes; earlier versions of Windows Server only note the attribute that was modified. And no version of Windows Server logs the prior value of changed attributes.

The limitations of Active Directory auditing become especially apparent with Group Policy Objects (GPOs). Misconfigured GPOs can quickly have devastating effects on multiple computers. However, the security log reports only that a GPO was modified; it provides no information about which of the hundreds of settings within a GPO were affected, or their before and after values.

Lack of Real-time Monitoring and Alerting

Windows Server provides no real-time monitoring or the capability to alert operations and security staff when high-impact changes or suspicious security events are detected. Windows Server 2008's Event Trigger capability could theoretically be used for this purpose, but event triggers are rudimentary at best and require significant scripting; the administrator must implement e-mail or pager notifications as well as workflow capabilities for tracking acknowledgement and resolution.

No Protection from Privileged Administrators

One key value of a monitoring and logging system is the deterrence gained by having a complete audit trail of actions performed by privileged administrators. However, since the native security log resides on the local file system of each domain controller, there is no protection of the audit trail from corruption or deletion by rogue administrators.

BRIDGING THE GAP: QUEST CHANGEAUDITOR FOR ACTIVE DIRECTORY

The Windows security log provides some functionality for monitoring changes in Active Directory, but there are significant gaps between the information you need and what the native security log actually provides. To bridge this gap, Quest provides Change Auditor for Active Directory.

Gaps and Limitations Addressed

The previous section identified seven critical problems with the Windows native security log that prevent organizations from meeting security and compliance requirements for Active Directory auditing and monitoring. Quest Change Auditor bridges all of these functionality gaps.

ACTIVE DIRECTORY LIMITATION	QUEST CHANGEAUDITOR FOR ACTIVE DIRECTORY CAPABILITY
No centralized audit trail	<p>ChangeAuditor agents on each domain controller efficiently send data to the ChangeAuditor server for consolidated analysis and reporting.</p> <p>Archived ChangeAuditor data can easily be accessed for future reporting and discovery needs.</p>
No reporting or analysis	<p>ChangeAuditor for Active Directory provides meaningful security and compliance reports on the fly. You can choose reports from the built-in compliance library or build your own reports. With ChangeAuditor, it is easy to prove compliance with standards such as SOX, HIPAA, Payment Card Industry Data Security Standards (PCI DSS), Federal Information Security Management Act (FISMA) and SAS 70.</p>
High volume of audit data	<p>ChangeAuditor’s configurable auditing allows administrators to enable or disable events from being generated. For example, you can opt to exclude high traffic or “safe” accounts from being audited in order to keep the audit database from growing too large.</p>
Performance risks	<p>ChangeAuditor captures Active Directory change information without the need for native audit logs, resulting in significant savings of storage and CPU resources.</p>
Missing or limited information	<p>ChangeAuditor tracks user and administrator activity in detail, including “who, what, when, where and why,” plus original and current values for all changes.</p> <p>ChangeAuditor provides audit visibility beyond native logs with coverage for GPO and nested groups. In addition, ChangeAuditor monitors changes to the registry, system services and local accounts that can indirectly have a high impact on both Active Directory and its underlying system security.</p>
Lack of real-time monitoring	<p>ChangeAuditor for Active Directory tracks critical configuration</p>

ACTIVE DIRECTORY LIMITATION	QUEST CHANGEAUDITOR FOR ACTIVE DIRECTORY CAPABILITY
and alerting	changes to your Windows environment, and then translates raw data into meaningful information. It offers real-time alerts, Smart Alert technology for intelligent event correlation, and in-depth reports on the activities taking place in your infrastructure.
No protection from privileged administrators	ChangeAuditor for Active Directory collects and stores your Active Directory audit trail on a separate system that can be protected from modification by AD administrators, so the integrity of audit trails is protected.

CONCLUSION

Because of its critical role in the enterprise environment, Active Directory requires careful monitoring and auditing. But native tools provide only limited audit capability, preventing organizations from meeting critical security and compliance requirements.

Quest ChangeAuditor for Active Directory bridges these gaps in functionality, enabling organizations to efficiently monitor high impact and suspicious Active Directory modifications and comply with regulatory and industry requirements.

ABOUT THE AUTHOR

[Randy Franklin Smith](#) is president of Monterey Technology Group, Inc. and creator of the [UltimateWindowsSecurity.com](#) Web site and training course series. Randy specializes in Windows security and is a [Systems Security Certified Professional](#) (SSCP), a Microsoft [Most Valued Professional](#) (MVP), and a [Certified Information Systems Auditor](#) (CISA). He is also the award-winning author of almost 300 articles on Windows security issues for publications such as [Windows IT Pro](#), for which he is a contributing editor and the author of the popular Windows Security log series. Randy can be reached at rsmith@ultimatewindowssecurity.com.

ABOUT QUEST SOFTWARE, INC.

Now more than ever, organizations need to work smart and improve efficiency. Quest Software creates and supports smart systems management products—helping our customers solve everyday IT challenges faster and easier.

At Quest, we focus on our customers first. Our products and people are dedicated to helping customers manage their critical applications, databases, Windows infrastructure and virtual environments. The combination of our award-winning software and strong customer relationships makes Quest a smart, reliable technology partner.

With consistent annual growth for 10 years, and 100,000 customers, Quest is a stable, global company that is positioned for long-term success.

Learn more at www.quest.com

Contacting Quest Software

Phone: 800.306.9329 (United States and Canada)

If you are located outside North America, you can find your local office information on our Web site.

Email: sales@quest.com

Mail: Quest Software, Inc.

World Headquarters

5 Polaris Way

Aliso Viejo, CA 92656

USA

Web site: www.quest.com

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a commercial version and have a valid maintenance contract. Quest Support provides around the clock coverage with SupportLink, our web self-service. Visit SupportLink at <http://support.quest.com>

From SupportLink, you can do the following:

- Quickly find thousands of solutions (Knowledgebase articles/documents).
- Download patches and upgrades.
- Seek help from a Support engineer.
- Log and update your case, and check its status.

View the ***Global Support Guide*** for a detailed explanation of support programs, online services, contact information, and policy and procedures. The guide is available at: [http://support.quest.com/pdfs/Global Support Guide.pdf](http://support.quest.com/pdfs/Global%20Support%20Guide.pdf)

NOTES

¹ COBIT, which stands for “Control Objectives for Information Technology,” was developed by the Information Technology Governance Institute (ITGI).