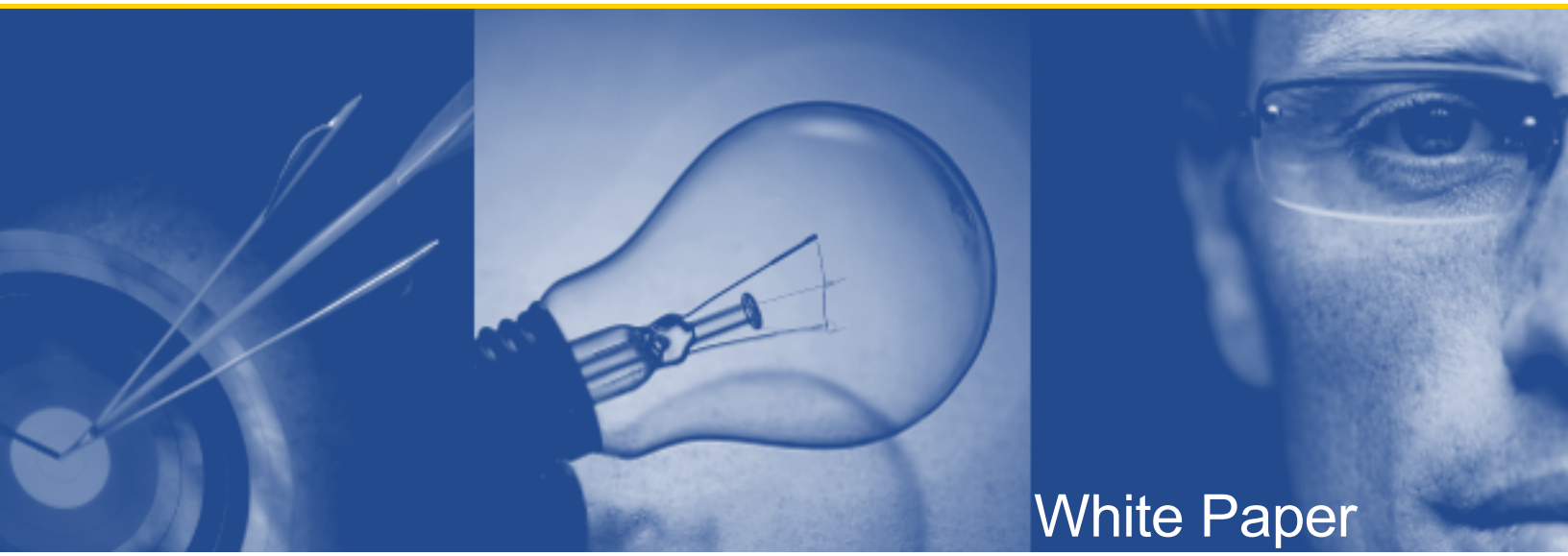
QUEST SOFTWARE®

Better Together: Auditing with Microsoft Audit Collection Services (ACS) and Quest Software

Written by
Tom Crane, Product Manager, Quest Software, Inc.

Edited by
James Galvin, Microsoft Sr. Product Manager, Microsoft



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

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—January, 2009

CONTENTS

INTRODUCTION

Microsoft has made great strides the last couple of years in enhancing its products to improve security. This white paper focuses on one of the most critical aspects of security: auditing and reporting for the Microsoft platform. It explains Microsoft's Audit Collection Services, a key feature in System Center Operations Manager 2007, and auditing enhancements in Windows Server 2008. Then it explains how Quest Software can complement Microsoft's solutions to provide extensive auditing and reporting across the entire IT infrastructure.

This white paper is written for IT managers, system administrators, security administrators, and others involved in the process of auditing their Microsoft applications, databases, and operating systems.

For the purpose of this white paper, auditing refers to the act of collecting, storing, alerting on, and reporting on events that are of significant importance to the IT infrastructure. Events can include general system activities such as modifications to critical system configurations and changes to access controls, as well as changes to password and group membership for sensitive accounts, and for inappropriate access to critical information. Many of these events are logged in their own audit trail, depending on the type of application, operating system, database, and device in use. Because the audit trails are siloed in nature, it's very challenging to aggregate, correlate, and report on the entire IT infrastructure in a holistic, efficient, and effective fashion.

In the pre-Sarbanes-Oxley (pre-SOX) era, auditing was considered optional by many organizations. A typical response to an auditing recommendation was, "Why would I want to know those details? That just raises more red flags that I don't have time to address." These days this response is not acceptable. Auditing is an absolute must to satisfy external regulatory requirements, standards imposed on organizations by partners, and internal security policies.

MICROSOFT'S AUDITING SOLUTION: AUDIT COLLECTION SERVICES (ACS)

Microsoft's auditing solution is System Center Operations Manager 2007, which gathers audit data from Windows systems through a feature called Audit Collection Services (ACS). This feature collects, consolidates, and reports on Windows security log data in near real-time with an extensible infrastructure designed to support enterprise compliance solutions.

Unlike traditional event and performance monitoring, in which administrators strive to gather only the events they need to take action on, ACS gathers all events written to the security log, because all security events are relevant to auditing, not just those that have a specific action required.

Architecture

Main Components

Operations Manager 2007 ACS comprises three components:

- The Audit Forwarder, which securely and efficiently forwards events from Windows systems to the central collector
- The Audit Collector, which consolidates the events received from the forwarders
- The Audit Database, which houses the collected events for reporting and analysis

The **Audit Forwarder** is deployed as part of the Operations Manager 2007 agent. By default, it is disabled, but it can be enabled from the Operations Manager console for systems that will be audited. By enabling the Operations Manager 2007 agent, the forwarder uses the agent's built-in security for communications with the server through a mutually authenticated, encrypted channel. This prevents tampering with the audit data being collected.

The **Audit Collector** is installed as an optional component on an Operations Manager 2007 Management Server. Each collector can handle many forwarders; the actual number will vary by the type of system being monitored and the mixture of system types, as well as the volume of events being audited in the audit policy. Customer usage data has shown that when using the default Windows Audit Policy, a single collector can handle 150 domain controllers (DCs) or 3,000 non-DC servers or 20,000 workstations. An Operations Manager 2007 Management Group can contain many Audit Collectors, depending on its capacity needs.

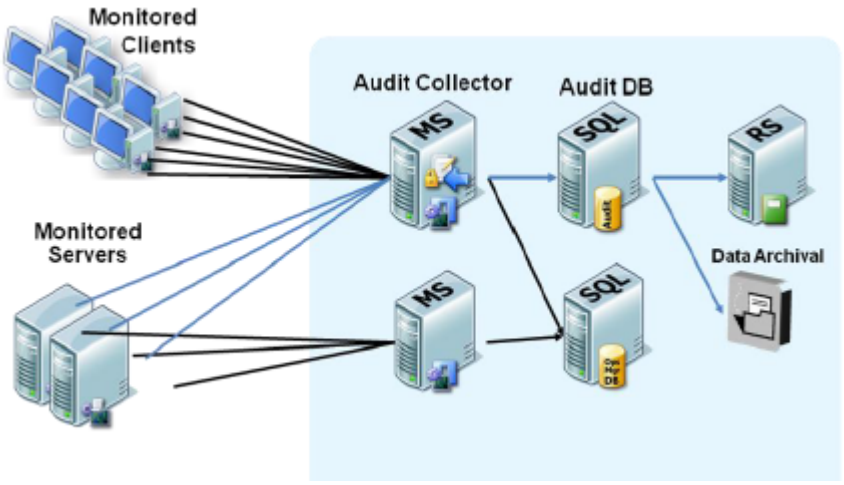


Figure 1. Operations Manager 2007 Audit Collection Services

The **Audit Database** is separate from the operations database and data warehouse used by Operations Manager 2007. This partitioning helps meet the data separation requirements of compliance rules and performance; often audit data is accessed by individuals who are not allowed access to operational data and vice versa. The Audit Database can share the same SQL Server instance if needed. A one-to-one relationship exists between the Audit Collector and the Audit Database. If multiple collectors are implemented, then multiple Audit Databases are required.

Expandable Platform

Audit Collection Services is an expandable platform within Operations Manager 2007. Certain core features of Operations Manager, such as reporting and event alerting, can also be used to improve visibility into the collected audit data.

A Windows Management Instrumentation (WMI) provider is included to allow rules to be created to monitor security log events. This provider allows management pack authors to create monitors that use audit data for tasks such as intrusion detection or forensics. In addition, the Audit Database has an open schema. These features allow developers to extend the Audit Collection functionality to meet specific audit data requirements, and Microsoft partners to build solutions for specific security and compliance needs.

Reports

Reporting for Audit Collection Services is built on SQL Reporting Services. Operations Manager 2007 includes several default reports that have been prebuilt for Audit Collection Services. Default audit reports include the following:

Account Management

- User account created/deleted, enabled/disabled
- Administrator groups changes
- Group membership changes
- Changing someone else's password
- Computer account created/deleted

Access Violations

- Unauthorized access attempts
- Account locked

Policy Changes

- Audit policy changed
- Object permissions changed
- Account policy changed
- Privilege added/removed

System Integrity

- Lost events
- Audit failure
- Log cleared

AUDITING WITH WINDOWS SERVER 2008

The Audit Collection feature of System Center Operations Manager 2007 is an easy-to-implement, secure, and efficient solution for collecting and consolidating audit data about events from multiple Windows systems. Let's take a closer look at the audit trail and some event-related enhancements introduced in Windows Server 2008.

Audit Trail Basics

An audit trail in the Microsoft Windows platform is synonymous with the Security event log, which captures the vast majority of events. Although the Windows Security event log normally audits simply whether each action was a success or failure, the sheer volume of events in the log makes identifying breaches a challenge. In particular, sophisticated attacks are often distributed across multiple systems, making analysis quite difficult.

The key elements that enable information to be recorded in the Security event log are Windows Audit Policy and system access control lists (SACLs).

The Windows Audit Policies define the collection of success and failure events for specific types of access. The following Audit Policy categories have been present in Windows for many years:

- 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

Most organizations define Audit Policy with these categories. However, two Audit Policy categories—Audit directory service access and Audit object access—rely on system access control lists (SACLs) to return information in the security event log.

What are SACLs? Each object (such as a file, registry entry, or directory service) has an access control list (ACL), which is a list of access control entries (ACEs). There are two types of access control lists:

- **Discretionary access control list (DACL)**
  A DACL specifies who is allowed or denied access to a securable object.

- **System access control list (SACL)**
  A SACL enables administrators to log attempts to access a secured object. Each entry (ACE) in a SACL specifies which types of access attempts by a specified trustee should be logged in the Security event log.

Understanding the relationship between Audit Policy and SACLs is critical because configuration is necessary to capture the "correct" audited events. That is, the audit directory service access and the audit object access policies enable the generation of audits in the Security event log for those categories of events, but events are generated only if an object has an auditing ACE configured in its SACL. Once these pieces are in place, security events are generated by the Windows Local Security Authority (LSA) and are written to the Security event log.

This type of auditing entails two problems: configuration must be performed on each object, and the auditing adds quite a bit of detail in the Security log and overhead on the servers. Windows Server 2008 addresses these challenges by introducing the Windows Eventing 6.0 event subsystem.

New Event Viewer User Interface

Included as part of this subsystem, Windows Server 2008 offers a new interface. The new Event Viewer Microsoft Management Console (MMC) snap-in has Overview and Summary pages, flexible custom views, and Explain Text. With these features, users can find event information and configure important event log options from the Event View itself.

In earlier versions of Windows, if scalability limits were exceeded, the entire logging process would stop—a real security issue. With Windows Eventing 6.0, logging is limited only by the amount of available disk space. Of course, large log files can be difficult to sort through, so the log must be maintained at a manageable size. To help, Windows Eventing 6.0 offers the “Archive the log when full, do not overwrite events” option, which helps to ensure events are archived on the local server.

However, Windows Eventing does not provide a solution for managing event logs over time or aggregating them for cross-system filtering and reporting; it is no substitute for a true log aggregator.

Another new capability of Windows Eventing 6.0 is associating administrative actions with specific events. This is accomplished by integrating the Windows Event Collector service with the Task Scheduler. The “Attach Task to the Event” wizard provides an easy way to start a program, send an email, or display a message any time a specific event is logged. These alerts are useful when specific changes can be pinpointed to a specific event, but correlating multiple events and parsing the contents of a specific event is best left to a real-time monitoring solution.

Granular Auditing Categories

Windows Server 2008 enables organizations to granularly control what events are written to the Security log. Previous versions of Windows had the nine audit categories listed earlier, but enabling them often resulted in information overload. Windows Server 2008 offers Granular Audit Policy: those nine categories are divided into 50 subcategories, enabling administrators to control what subsets of events are recorded. This reduces the overall amount of audit information collected.

Change Management Details

Windows Server 2008 also improves change management. Previous versions of Windows recorded only basic details, such as the Active Directory object attribute or registry value that was changed. The Windows Server 2008 auditing subsystem captures both old and new values in the security log for specific objects. This capability applies only to Active Directory Domain Services, Active Directory Lightweight Directory Services, and registry.

To record these details, enable Audit Success or Audit Failure on the subcategories for “Registry” or “Directory Service Changes” and set the associated SACLs. Two entries will be written, one for the value being deleted and another for the value being added (unless the attribute was blank, in which case only one entry is made, for the value being added). Setting up the capture of this granularity of detail, however, is an arduous task that must be well planned out.

Event Subscriptions

A new feature of Windows Server 2008 is Event Subscriptions, which provides a way to forward events directly between systems. It consists of an Event Collector that gathers events, and Event Sources that are configured to forward events to specified hosts. The collected events are written to the ForwardedEvents event log on the collector. Although this feature is satisfactory for managing a few systems, it’s not a solution for log aggregation across multiple servers.

Object Protection

Windows Server 2008 exposes the ‘Protect object from accidental deletion’ option in the Active Directory Users and Computers MMC. This capability has been available since Windows 2000 but now it’s easier to implement. This option prevents an organizational unit (OU) from being accidentally deleted or moved—changes that could result in disruption of services or downtime. Although protecting OUs is much simpler now, protecting sensitive security groups, users and Group Policies still requires setting the SACLs on the objects. Preventing attribute-level modifications is not possible.

QUEST AUDITING SOLUTIONS

With the wealth of features and the enhancements in Windows Server 2008, System Center Operations Manager is an easy choice for organizations that have many systems to manage. And because Operations Manager can accept data from other sources, administrators can use other solutions for help in managing their heterogeneous environments while maintaining Operations Manager as the central interface.

Quest provides a variety of products that easily interface with Operations Manager and ACS to satisfy enterprise reporting and auditing needs. Quest solutions securely collect, store, report on, and alert on heterogeneous event data and configurations to meet the needs of external regulations, internal policies, and security best practices.

InTrust

To fulfill enterprise auditing and reporting needs, Quest InTrust collects, stores, reports and alerts on event data from Windows, Unix, Linux, ACS databases, and syslog devices. With its family of plug-ins, organizations can granularly audit and prevent changes to Active Directory objects, Group Policies, files and folders, and Exchange mailboxes. Without native auditing being enabled these products capture 'who' made the change, 'what' object was changed, 'what' the before and after values are, 'where' it originated, and 'when' it occurred. Compliance officers, auditors and administrators can leverage this family of solutions to manage a wide range of platforms and reduce the complexity of audit log management. Key architecture features reduce expensive storage overhead and administration costs as well as provide a scalable solution for long-term enterprise storage.

InTrust Plug-in for Active Directory

InTrust Plug-in for Active Directory provides granular auditing, reporting, and alerting on all changes to Active Directory objects and Group Policies, in addition to other domain controller activities. Administrators can troubleshoot AD problems and reverse any changes, if necessary, or for the most sensitive areas, they can revert changes automatically. InTrust Plug-in for Active Directory also provides protection against changes to the most critical AD objects, such as organizational units (OUs) being accidentally deleted and GPO settings being modified.

InTrust Plug-in for File Access

InTrust Plug-in for File Access provides real-time, detailed tracking of all user and administrator file and object access activity on Windows file servers. It provides efficient collection and storage of audit data and enables organizations to effectively react to—and even prevent—access and permission changes in their file server configurations.

InTrust Plug-in for Exchange

InTrust Plug-in for Exchange provides comprehensive activity tracking and mailbox access auditing for Microsoft Exchange servers. The solution allows organizations to track, store, alert on, and report on Exchange server activity and non-owner mailbox access, which improves security and reduces compliance risks.

ChangeAuditor

Quest ChangeAuditor offers a family of easily installed and implemented solutions. ChangeAuditor proactively listens for changes to Active Directory, file systems and Exchange, and provides administrators with audited event data in real time.

ChangeAuditor makes Windows auditing much easier because:

- Similar change events are captured even if the Security log rolls over
- All events are detailed so administrators will know exactly what happened
- All events contain the pre and post value of the change

ChangeAuditor for Active Directory proactively tracks, audits, reports on, and alerts on vital configuration changes—in real time and without the overhead of native auditing. You'll instantly know who made what change when, where, and why.

ChangeAuditor for File Systems drives the security and control of file systems by tracking all key file and folder changes in real time. With ChangeAuditor for File Systems, you'll get the "Who, What, When, and Where" of each change, the previous and changed values, and comments on why the change was made.

ChangeAuditor for Exchange proactively audits the activities taking place in your Exchange environment and provides real-time, in-depth tracking, as well as detailed alerts about vital changes that occur. You can audit changes to non-owner and owner mailbox access, administrative groups, mailbox policies, public and private information store, organizational changes, distribution list changes, and more.

The Quest granular auditing solutions for Active Directory, Exchange, and file servers aggregate their information into one central location for enterprise-wide reporting on changes such as Group Policies links, users created or deleted, schema changes, mailbox accesses and permissions being changed. These solutions do not depend on native audit policies being enabled or on native event logs. In addition to capturing all changes, these solutions enrich the events with before and after values and display this information in easily understandable terms. All events are designed to capture who made the change, what was changed, where it occurred and when it happened.

Solutions that Provide Integration with ACS

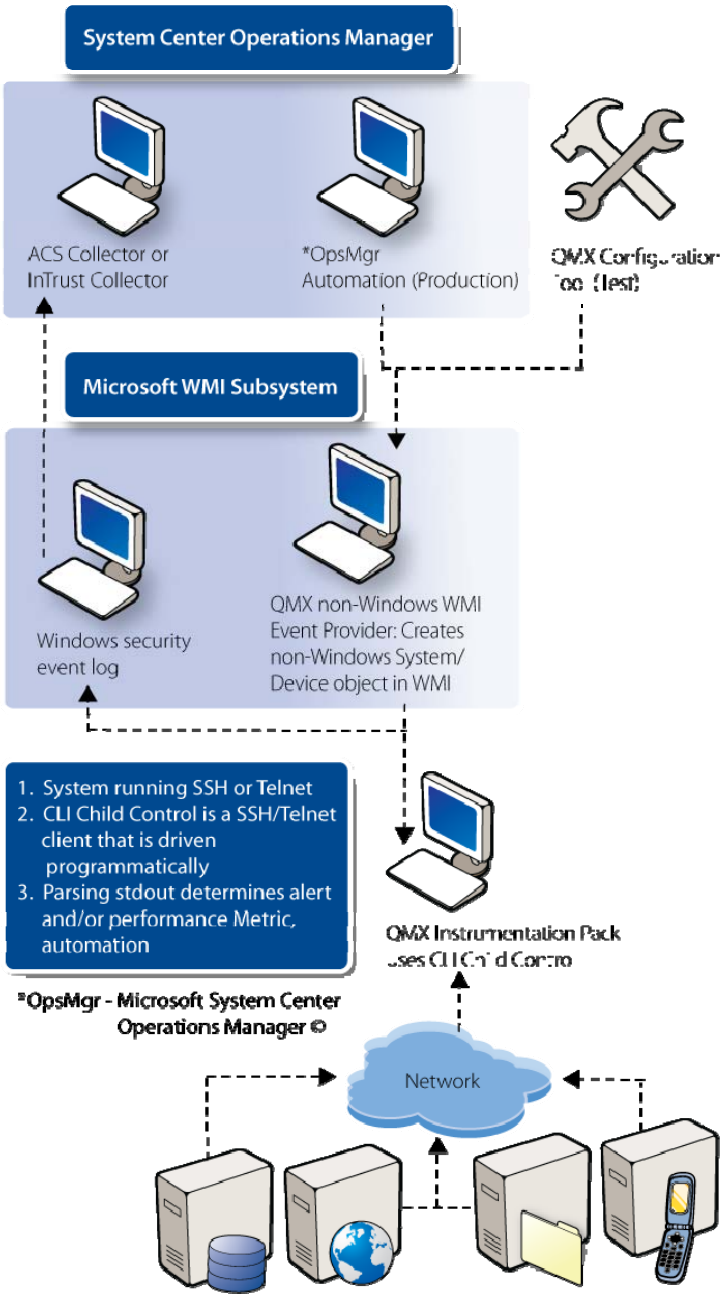
Quest has multiple solutions that provide seamless integration with Microsoft's System Center Operations Manager and Audit Collection Services (ACS).

- **Quest ReportADmin for ACS** is a free solution that provides consolidated reporting within a single reporting database. From a single console administrators can configure multiple ACS collectors and create custom filters to determine which events are sent to the central reporting database. It includes a built-in report library and custom reporting templates, along with Microsoft SQL Reporting Services (SRS) for automated report generation and delivery. Download a copy today at http://www.quest.com/reportadmin-for-acs/.
- **Quest Knowledge Pack for ACS** uses InTrust to collect ACS audit data, providing an efficient long-term storage solution and deep correlated enterprise reporting.
- **Quest Management Connector for InTrust** enables heterogeneous audit and compliance alerts to be sent through Operations Manager 2007.
- **Management Pack for ChangeAuditor** sends user defined events to the Operations Manager database. Administrators can then take the real-time information from ChangeAuditor and find the corresponding event log information in Operations Manager's auditing component.

Quest Management Xtensions

ACS includes capabilities for collecting short-term and long-term data, inserting it into a well-designed database schema, and reporting on it relating to security events. Using the architecture of ACS allows Quest to integrate security events from non-Windows infrastructure into its stream. In order to maintain the integrity of the ACS architecture, all of the non-Windows security events are collected into the security logs of the ACS collection server, and the ACS process flow carries out the insertion of those events into the standard schema, which allows for ease of integration, compliance and reporting.

Quest Management Xtensions—Operations Manager 2007 Edition (QMX) collects non-Windows security events and feeds them into the ACS dataflow. QMX is designed to handle any alert data defined by QMX out of the box, as well as alert data deemed to be security events by the user. The non-Windows data can come in from any communication protocol or service method used to monitor any given infrastructure component supported, including web services, ssh, telnet, snmp, api, and direct DB calls. With QMX and Microsoft ACS, you have a standard process for capturing, compiling, storing, and reporting on all infrastructure components across the global enterprise.

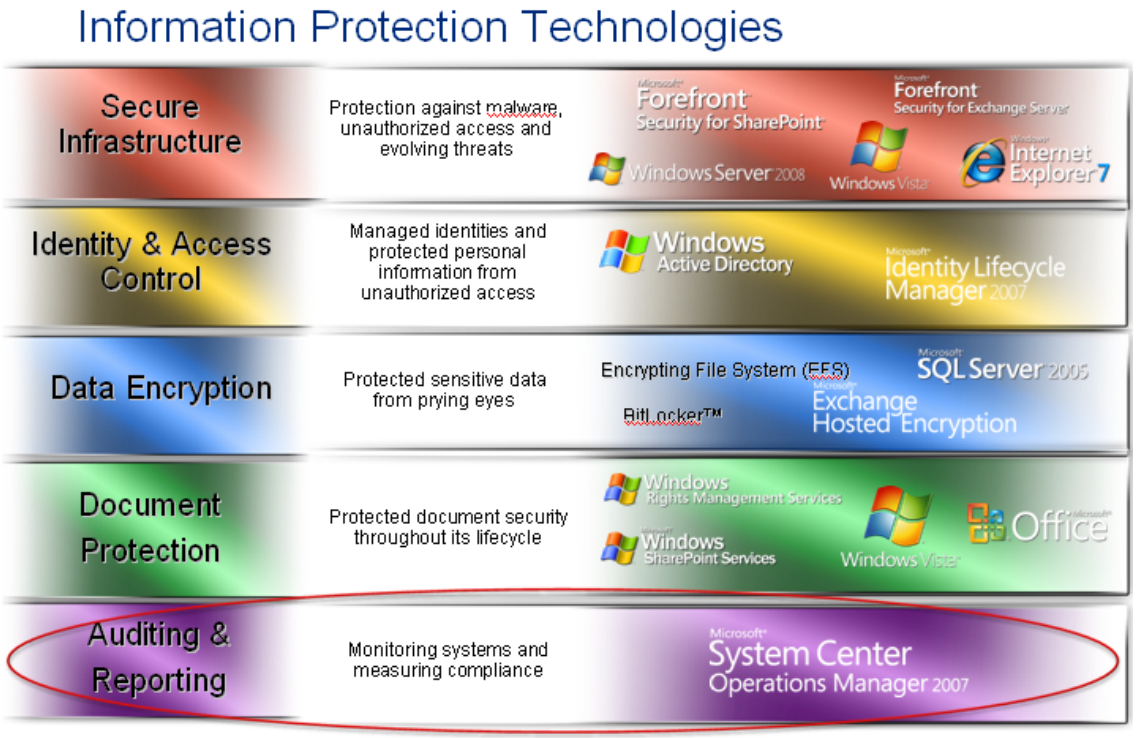

System Center Operations Manager
ACS Collector or InTrust Collector
*OpsMgr Automation (Production)
Microsoft WMI Subsystem
Windows security event log
QMX non-Windows WMI Event Provider: Creates non-Windows System/ Device object in WMI
1. System running SSH or Telnet
2. CLI Child Control is a SSH/Telnet client that is driven programmatically
3. Parsing stdout determines alert and/or performance Metric, automation
*OpsMgr - Microsoft System Center Operations Manager ©
Network

How Quest and Microsoft Audit Better Together

As discussed earlier, Audit Collection Services provides Microsoft customers with an easy-to-implement, secure, and efficient solution for collecting and consolidating audit data from multiple Windows systems, but gaps in ACS must be addressed when customers seek a compliance solution. This section explains how customers will gain additional value by using the strengths of both Microsoft and Quest when addressing auditing requirements.

Summary of Microsoft Strengths

Beyond auditing and reporting, Microsoft offers numerous technologies to address other information protection issues such as secure infrastructure, identity and access control, data encryption and document protection. The figure below illustrates how Microsoft addresses some of the most important issues for organizations today.



System Center Operations Manager 2007's Audit Collection Services Microsoft provides the following benefits:

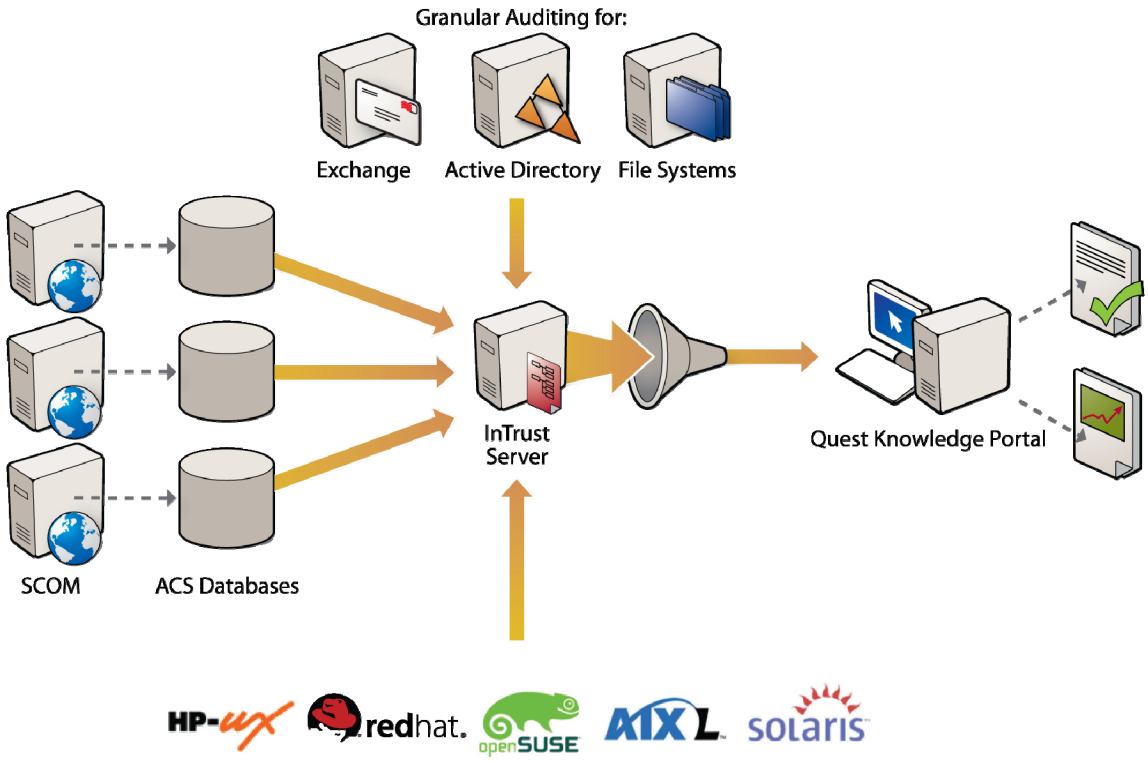
- Near real-time collection of all events written to the Windows security log
- Expandable platform with Windows Management Instrumentation (WMI) provider, which allows the creation of custom rules to monitor security events
- An auditing database with an open schema, which allows developers to extend functionality to meet specific audit data requirements
- Uses SQL Reporting Services
- Secure, efficient, and scalable architecture for enterprise customers
- Integration with System Center Operations Manager
- Single agent for both monitoring and forwarding to audit collection services
- Costs are included in the System Center Operations Manager 2007 Operations Management license
- Alerting on security events

Summary of Quest Strengths

Customers who use Microsoft System Center Operations Manager with Audit Collection Services benefit from Quest solutions with:

- Reduced complexity when configuring Windows systems to create a relevant audit trail
- Rich auditing details with minimal performance burden
- Proactive enforcement capabilities that prevent unwanted changes
- Forensic capabilities and accurate efficient event data retention
- Extensive coverage that extends beyond the Microsoft platform

The following diagram illustrates the advantages of using both Microsoft and Quest solutions together:



CONCLUSION

Microsoft greatly improved its auditing and reporting solution with the introduction of System Center Operations Manager 2007 Audit Collection Services. Significant additional enhancements were included in the Windows Server 2008 operating system, including the new event subsystem.

Microsoft has significantly increased the auditing and reporting capabilities of System Center Operations Manager with ACS, which further enables complementary solutions from third-party software vendors like Quest Software to add value to the enterprise security and compliance solution. Quest solutions expand coverage beyond the Microsoft platform; provide richer change details, enhanced forensic capabilities, and proactive enforcement to ensure changes cannot be made unless authorized. The combination of Microsoft and Quest auditing solutions provide a truly comprehensive set of capabilities.

ABOUT THE AUTHOR

With more than thirteen years of experience working in the areas of Active Directory, Exchange and SQL management and compliance, Tom Crane is the Product Manager Quest's Active Directory, Exchange, File Server, Windows and Unix auditing solutions. He is responsible for technical direction and field execution of these solutions. Prior to this position he managed the architecture specialists in the compliance area.

Prior to Quest, Tom worked for a division of News Corporation and financial institutions. He has a degree in Philosophy from Northern Illinois University and a Masters degree in Computer Information Systems from Northwestern University.

ABOUT QUEST SOFTWARE, INC.

Quest Software, Inc., a leading enterprise systems management vendor, delivers innovative products that help organizations get more performance and productivity from their applications, databases, Windows infrastructure and virtual environments. Quest also provides customers with client management through its ScriptLogic subsidiary and server virtualization management through its Vizioncore subsidiary. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 100,000 customers worldwide meet higher expectations for enterprise IT. Visit www.quest.com for more information.

Contacting Quest Software

Phone:	949.754.8000 (United States and Canada)
Email:	info@quest.com
Mail:	Quest Software, Inc. World Headquarters 5 Polaris Way Aliso Viejo, CA 92656 USA
Web site:	www.quest.com

Please refer to our Web site for regional and international office information.

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