Microsoft® SystemCenter

Audit Collection with Microsoft® System Center Operations Manager 2007

Microsoft Corporation

Published: December 18, 2006
Updated: December 18, 2006

Executive Summary

Supporting business efforts to comply with Federal Regulations with acts such as Sarbanes-Oxley or HIPAA is a requirement for many IT organizations. One of the most difficult steps in implementing compliance solutions is the gathering of security audit data from the many distributed computers systems covered by the regulations. System Center Operations Manager 2007 helps in the process of gathering audit data from Windows systems through a feature called Audit Collection Services. Audit Collection Services collects, consolidates, and reports on Windows security log data in real-time with an extensible infrastructure designed to support enterprise compliance solutions.

This document is developed prior to the product's release to manufacturing, and as such, we cannot guarantee that all details included herein will be exactly as what is found in the shipping product. The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication. The information represents the product at the time this document was printed and should be used for planning purposes only. Information subject to change at any time without prior notice. This whitepaper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

Contents

Contents 3

Introduction 4

System Center Operations Manager 2007 4

Audit Collection 4

Operations Manager 2007 Audit Collection Services 5

Audit Reporting 5

Audit Collection Architecture 6

More Information 7

Introduction

In today's enterprise IT environment pressures come from many different sources, end-users, the business, industry trends, and government regulations. One of the most difficult pressures for an IT organization to manage is the need to keep systems running efficiently while adhering to increased security and regulatory requirements. Being able to keep IT services running while gathering the data need to satisfy regulators and business stakeholders is crucial the success of an IT organization.

Windows systems are a critical platform that IT organizations need to audit and report on for security and compliance. Gathering all the data from the many distributed Windows member servers, clients and Active Directory domain controllers can be a daunting task. Questions like 'How to access the data securely?', 'Once accessed, how do you transport and store the audited data?', and 'How do you report what you have in a meaningful way?' , must be answered. In the past this has often been an expensive and custom solution which takes a great deal of effort to implement. With the introduction of the Audit Collection feature of System Center Operations Manager 2007 Microsoft is providing an easy to implement, secure and efficient solution for collecting and consolidating audit data from multiple Windows systems.

This paper provides a high-level overview of the Audit Collection Services feature of System Center Operations Manager 2007.

System Center Operations Manager 2007

System Center Operations Manager is a software solution designed to meet the need for end-to-end service monitoring in the enterprise IT environment. System Center Operations Manager provides an easy-to-use monitoring environment that monitors thousands of event and performance counters across hundreds of operating systems and applications to provide a single view of the health of an organization's IT environment. This view of a service's health is key to a rapid, agile response to events that may impact the normal running of a business and ultimately cost an enterprise money.

System Center Operations Manager 2007 is the third version of Microsoft's award-winning monitoring solution. Operations Manager 2007 builds on the success of its predecessors by adding key features and functionality that customers and the market have been demanding. Microsoft listened to users of the first two versions of Operations Manager to find out what they liked, and what they didn't like. Customers said they wanted to monitor more than just individual servers, they wanted it to be easier to find computers and applications that need to be monitored, and they wanted more detailed troubleshooting and best practice knowledge. The market for management solutions also played a part in the design of Operations Manager 2007. More enterprises are implementing Service Level Management, and more companies are finding a need to monitor their ever-expanding network of Microsoft Windows-based systems.

To respond to these needs, Microsoft enhanced the already capable Operations Manager solution by designing Operations Manager 2007 around these three pillars:

- End-to-end service monitoring
- Best-of-breed manager of Windows
- Increased efficiency and control

Within these pillars, Microsoft has leveraged the best of existing technologies, such as Windows and Microsoft SQL Server, and has embraced new technologies, such as the System Definition Model (SDM) and the Windows PowerShell scripting engine. System Center Operations Manager 2007 has answered the IT service management needs of both customers and the market.

Audit Collection

The implementation of regular system auditing is an important best practice in IT organizations for reasons such as operations security or regulatory compliance. In a Windows system, an audit policy configures which events are recorded to the Windows security log. This log of audit data must then be analyzed and reported on to gain any insight into the information. To do this for Windows systems on an enterprise-wide scale, a system is needed to collect, consolidate, analyze, and report on audit data for many distributed systems. Operations Manager 2007 and includes the Audit Collection Services feature, which automates the collection and consolidation of Windows security logs.

Windows provides an extensive list of auditable events that can be captured in the Windows security log, such as account management events, access violations, policy changes, and system integrity. Audit policy design should be done carefully because auditing too much can be just as bad as auditing too little. Audit logs can quickly become too cumbersome to manage if nonessential events are included in the policy.

The most pressing reason for audit collection within an enterprise is the need to meet specific regulatory compliance requirements, such as Sarbanes-Oxley Act or HIPAA regulations. Audit Collection Services, such as those in Operations Manager 2007, are a small but crucial part of an overall compliance solution. Audit Collection Services gather the required data to be analyzed against the specific compliance rules. Although no tool or technology can provide a complete compliance solution, tools such as Operations Manager 2007 can provide solutions to specific compliance challenges, such as data gathering.

Operations Manager 2007 Audit Collection Services

Audit Collection is a feature of Operations Manager 2007 that allows events written to the security log on Windows systems to be collected and consolidated in near real-time. Audit Collection is different from traditional event and performance monitoring, in which administrators strive to gather only the events they need to take action on. Audit Collection necessitates the gathering of all events written to the security log because all security events are relevant to auditing, not just those that have a specific action required.

Audit Reporting

Reporting for Audit Collection is built on SQL Reporting Services. Operations Manager 2007 includes several default reports that have been prebuilt for Audit Collection. 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 Violation

- 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

Like all reports in Operations Manager 2007, the default Audit Collection reports can be modified. However, audit reports are modified using SQL Report Builder, not the reporting section of the Operations Manager 2007 console. This separation allows Audit Collection reports to be owned and accessed by individuals who do not have access to regular operational data through the Operations Manager 2007 console.

Audit Collection Architecture

Operations Manager 2007 Audit Collection is made up of 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; and the Audit Database, which houses the collected events for reporting and analysis. In addition to these components, Operations Manager core features such as reporting and event alerting can be used to enhance the visibility into the audit data collected.

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 leveraging 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 amount of events being audited in the audit policy. Customer usage has shown when using the default Windows Audit Policy a single collect can handle 150 Domain Controllers (DC) or 3,000 non-DC servers or 20,000 workstations. An Operations Manager 2007 Management Group can contain many Audit Collectors depending on the capacity needs.

The Audit Database is separate from the operations database and data warehouse used by Operations Manager 2007. This partitioning helps with meeting 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 will be required.

Audit Collection is an extensible platform within Operations Manager 2007. A Windows Management Instrumentation (WMI) provider is included to allow rules to be created to monitor security log events. This provider will allow management pack authors to create monitors that use audit data for tasks such as intrusion detection or forensics. In addition to the WMI provider, the Audit Database has an open schema , these features allow developers to extend the Audit Collection functionality to meet specific audit data requirements. Microsoft partners are using these features to build solutions for specific security and compliance needs.

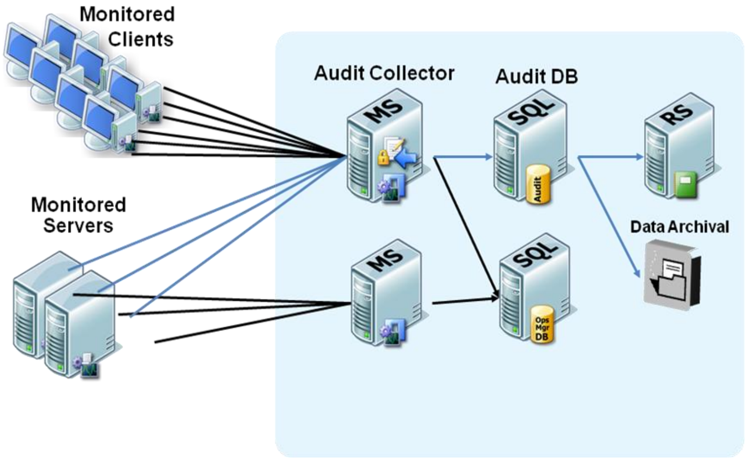

Figure 1 - Operations Manager 2007 Audit Collection Services

More Information

Operations Manager 2007 provides extensive support documentation around configuring and enabling Audit Collection Services with the product help file.

System Center Operations Manager 2007 information is available online at http://www.microsoft.com/opsmgr.

For support, newsgroups, blogs, and Knowledge Base articles, visit the Operations Manager Community Page at http://www.microsoft.com/mom/community.

Additional information on the Microsoft System Center family and DSI vision is at http://www.microsoft.com/dsi and http://www.microsoft.com/systemcenter.