Client Monitoring with Microsoft® System Center Operations Manager 2007

Microsoft Corporation

Published: December 18, 2006

Updated: December 18, 2006

Executive Summary

Client monitoring is a new feature of System Center Operations Manager 2007. By extending the award-winning monitoring capabilities of Operations Manager from servers to clients, Microsoft is providing a new level of visibility into the operations and efficiency of enterprise IT environments. This paper outlines the client monitoring capabilities of Operations Manager 2007.

Contents

Introduction

These days IT departments are under intense pressure—pressure from users who want more productivity and from business groups who want to see more value. Pressure also comes from regulators demanding compliance, technology advances, and from competitors. IT departments must manage these pressures to keep their businesses running while lowering costs. The bulk of many IT budgets are spent "treading water," simply maintaining the current systems and services. Only a small fraction of an IT budget is spent on new technologies and services that can move the business ahead. The cost of hardware and software is tracking downward, but the cost of managing and operating these assets is increasing. By gaining an upper hand in monitoring and managing their IT services, like desktop and mobile clients, IT departments can do more with fewer resources, manage the complexity of their environment, and achieve the agility necessary to be successful. Traditionally, client computers are ignored by enterprise IT departments. They are considered non-critical and do not warrant much attention from administrators. End-user productivity was not as important as the efficiency of the back-office servers, which were viewed as running the business. As technology changes, so does the role of the client computer. Desktops and mobile computers are now a critical part of any business, and almost every business relies on a client computer as much as they do their servers. Client computers run the point-of-sale devices in retail stores, they operate automated bank machines, and they allow countless millions of employees to access information and communicate with each other. In today's world, the client computer is critical to the business.

With the client's move to critical status, the need to monitor them has grown dramatically. Just as with servers, administrators need to know how the health and performance of client systems when problems arise. The more proactive that an administrator can be, the more efficient and productive the client systems can be. Client monitoring is flexible, and administrators can apply as much or as little as needed to meet their organizations' needs. For example it may be appropriate to simply monitor the systems for application crashes and then report on the crash or full agent monitoring of individual systems (similar to how servers are managed) may be needed.

Microsoft System Center Operations Manager 2007 launches Microsoft's effort into end-to-end service monitoring of client computers. Microsoft is no stranger to client management. Products like System Management Server (SMS) have been used for years to manage client computers' configurations. Operations Manager 2007 introduces event and performance monitoring of client computers to the capabilities of the Microsoft System Center family of management solutions.

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 events 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 did notlike. 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 this need, 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 embraced new technologies, such as the System Definition Model (SDM) and Windows PowerShell scripting engine. System Center Operations Manager 2007 has answered the IT service management needs of both customers and the market.

Client Monitoring

Monitoring of computer systems is not a new concept; servers have been monitored since their creation. Monitoring can be as simple as detecting whether the system is turned on or as complex as knowing the exact performance of a specific application or service running on the system. Monitoring has evolved over the years to incorporate very complex processes and metrics to support different needs of IT administrators. The nature of monitoring incurred an additional cost to running the system. This cost was often not economical to apply to client systems owing to the sheer numbers of clients versus that of servers. The time and money needed to monitor a server was offset by the productivity lost by the company if the server was not performing correctly. Client systems are most often used by one person. The impact of a single user's productivity loss is not usually noticeable. Some client systems such as Kiosks, Automated Bank Machines, or Point of Sales systems are different, and in the past they have been monitored similar to servers.

Clients computers are becoming more important in today's IT environment. Servers are no longer the sole location for critical data and process execution. Applications such as messaging and collaboration are now critical to the success of many organizations. Client's computers are critical parts of these and many other business applications and the need to monitor them is more important than ever. If a users' client systems is not functioning, they cannot communicate or access information critical to their and the organization's success. Simple disruptions like the time spent waiting for an application to restart after a crash or the inability to connect to an e-mail server are a nuisance to one user, but when they occur frequently across all client systems they have a dramatic impact on productivity similar or greater to that of a server outage.

Today, 90 percent of application crashes go unreported. Users simply reboot the application and continue working. The remaining 10 percent are either solved by the helpdesk using a known fix or escalated to specialists for resolution. Often the fix requires a reboot because not enough information is known about the crash to diagnose the problem. Effective client monitoring of application crashes can not only catch these unreported problems but also provide enough detail to determine why the application crashed in the first place.

In System Center Operations Manager 2007, client monitoring is applied in a flexible approach. The first level is Crash and Hang Monitoring in which client systems are monitored for application crashes. When a crash is detected, the crash information, including memory dumps, can be sent to the Management Server for storage. This crash information can be used for alerting or reporting purposes to determine problems or trends. The second and third levels of monitoring involve the use of an Operations Manager agent in which a management agent is installed on the client and more information is gathered or monitored. The difference between level 2 and level 3 is the focus of the monitoring. Level 2, or Collective Health Monitoring, views the client environment in collective groups. Based on events and performance data gathered in an aggregated fashion, administrators can view trends across different groups of clients. Level 3, or Business Critical Monitoring, is similar to server monitoring in that events and performance data are gathered on individual machines and not groups of machines. An organization may implement any combination of the different levels to fit its needs. For example, all client computers may be monitored to level 1, but only a small percentage may be involved in Level 2 and an even smaller percentage are critical enough to warrant level 3.

The effort required to implement and monitor a client increases as the levels go up.

Agentless Monitoring

If a management agent is not deployed to the client system being monitored, it is referred to as agentless monitoring. Agentless monitoring imposes restrictions on what can be monitored. In Operations Manager 2007, agentless monitoring monitors only application crashes and hangs through the feature Agentless Exception Monitoring (AEM).

Crash and Hang Monitoring

AEM gathers application crashes and hangs from Windows operating systems and the applications running on them. All supported Windows operating systems have a service called Windows Error Reporting. Windows Error Reporting uses the Windows Error Reporting client, also known as the Watson client, to gather information about application and operating system crashes. AEM can then forward the crash information to Microsoft for analysis.

Operations Manager 2007 allows Windows Error Reporting to first forward those errors to a management server operated by the organization. Figure 1 shows the communication channels for sending crash and hang data to Operations Manager and to Microsoft. Administrators can decide if they want to send the data to Microsoft for analysis and to see if a resolution exists. Having access to this information provides administrators with visibility into errors they have never had before. AEM offers the flexibility of sending no information, error IDs only, or full crash information, including memory images, for analysis. If an error ID or full crash information is sent, Microsoft will search its knowledge base of errors and return a resolution if one exists. Microsoft uses crash information to improve the quality of its products. By having access to this crash data, administrator's can use it to improve the quality of their own internal applications as well.

Agentless Crash Monitoring requires very little overhead and because crashes happen infrequently, it can easily be deployed across all of the client systems within an enterprise without a large data storage burden.

Reporting

Crash and hang monitoring in Operations Manager 2007 includes several pre-built aggregate reports which are available through Operations Manager 2007's reporting solution. Reports allow administrators to focus their attention on problem areas which may not be reported to the helpdesk by end users. Others reports include error trends by application and cost incurred due to errors and system crashes.

Agented Monitoring

Agented monitoring, as the name implies, involves the deployment of a software agent to the client computer that will be monitored. The agent monitors performance and events. It applies configured rules to determine events that need to be collected and alerted on. Agented Monitoring also allow tasks to be executed locally to correct problems or gather additional information as required.

Operations Manager 2007 implements a flexible approach to agented client monitoring. Agented monitoring can be performed on groups of client systems or on individual systems. Collective Health Monitoring monitors devices individually, but the reports and alerts are based on aggregate data across a group of systems. Business Critical Monitoring for client systems uses the same method that Microsoft does to monitor its servers, with each system being alerted and reported on individually.

Collective Health Monitoring

Agentless Crash Monitoring gathers only application and system crashes, so this information does not provide any insight into the availability or performance of an organizations' client systems. To gain this level of insight, administrators need to deploy an agent that can gather performance data.

Collective Health Monitoring is performed by gathering event and performance data from many machines and aggregating the data together based on groups of systems for reporting and analysis. For example, individual memory performance data is gathered from Windows XP and Windows Vista clients on different types of hardware. Collection Health Monitoring will aggregate this data together and provide reports based on memory performance for specific groups of systems, such as by operating system or by hardware vendor. This makes analysis of overall performance easier than digging through long lists or individual system performance reports.

Operations Manager 2007's monitoring agent will run on client operating systems. This agent can use the same Management Packs as the server agent and can also support the Audit Collection features of Operations Manager 2007. The agent and AEM can be combined to provide a complete monitoring experience. Operations Manager 2007 will provide management packs for the client operating systems and information worker applications, such as Microsoft Office. These management packs are specially designed for client monitoring and offer the ability to tuned for either Collective Health Monitoring or Business Critical Monitoring. See the Client Operating System Management Packs and Information Worker Management Pack sections of this paper for more information.

In most cases, an organization will deploy Collective Health Monitoring to portions of its client installed base. Agented monitoring will increase the amount of data being stored in both the Operations Manager operations database and reporting data warehouse due to the increased number of systems being monitored. The amount of data per system, however, is much lower than what would be retained due to Business Critical Monitoring or Server monitoring. An organization will likely select a representative cross-section of its client base for Collective Heath Monitoring.

Business Critical Monitoring

In some cases, client systems are critical to the business' operations. Point-of-sale terminals, kiosks, bank ATMs, or certain employee workstations, such as bank traders or manufacturing engineers, are examples of critical client systems. If a critical client system goes down or has significant performance problems, the business will lose money. These systems need to be monitored as if they were servers.

User Perspective Monitoring is an important part of IT service monitoring. Administrators need to understand the experience an end user has when interacting with an IT service they are offering. Business Critical Monitoring allows clients to be deployed as watcher nodes and run synthetic transactions against IT services.

In addition to event and performance data, oftentimes business critical systems require audit collection to ensure that compliance requirements are met. Business Critical Monitoring can use the Audit Collection features of Operations Manager 2007 for this purpose.

Business Critical Monitoring uses the same agent as Collective Health Monitoring; the management packs are simply tuned differently for the critical systems to allow for the individual alerting and reporting. See the Client Operating System Management Packs and Information Worker Management Pack sections of this paper for more information.

Business Critical Monitoring is usually a small subset of the client systems in an organization. Depending on the amount of information being monitored, the storage requirements for monitoring data can be similar to that of a server. System Center Capacity Planner can determine the correct Operations Manager configuration based on the organization's specific needs for Client Monitoring.

Reporting

Reporting on Agent monitored clients will vary depending on the management packs deployed and the level of client monitoring employed. Collective Health Monitoring uses aggregate data to provide reports for groups of systems. Business Critical Monitoring provides individual system reports similar to that of servers. Client systems are represented in Operations Manager the same way as servers so that administrators can leverage any of the generic reports provided by Operations Manager for client reporting. Reports are included as part of the management pack, so for more information on specific client management pack reports, see the Client Operating System Management Packs and Information Worker Management Pack sections of this paper.

Client Monitoring Architecture

Operations Manager 2007 employs several architectural components to enable client monitoring. Client monitoring consists of a management server, two agents, and a communication channel.

The management server is the same server used by Operations Manager for various kinds of monitoring for all servers or clients. The management server communicates with the agent and forwards events and performance data to the operations database. A management servers can be used for both server and client monitoring at the same time. Similar to server monitoring in Operations Manager 2007, Gateway servers can be used to monitor clients in untrusted domains or behind firewalls. Gateway servers, however cannot be used for enabling AEM.

Operations Manager 2007 leverages two agents for client monitoring. For Agentless Crash Monitoring to function, Operations Manager uses the existing Windows Error Reporting or Watson client, which is part of the Windows operating system. For Collective Health or Business Critical Monitoring, Operations Manager employs its own agent. The Operations Manager monitoring agent runs locally on the client system and provides event and performance data gathering, task execution, and audit collection functions to Operations Manager.

The communication channel between the management server and the agents is secured by default. The agent and management server mutually authenticate each other before communication can occur. This authentication uses Kerberos by default but can be configured to use certificates as well. The management server/agent traffic is encrypted to prevent tampering.

Operations Manager 2007 leverages Active Directory extensively for client monitoring. Active Directory is used for discovery of clients to be managed, for authentication of server agent communications, and for authentication of administrators authorized to monitor clients in Operations Manager.

Like server monitoring, client monitoring with Operations Manager 2007 requires the use of management packs. Management packs are collections of knowledge, monitors, rules, and reports specific to a technology to be monitored. Client-specific management packs exist for operating systems and applications. Management packs are provided by Microsoft and Microsoft partners, or they can be customer-built by IT administrators. Management packs provide Operations Manager with the knowledge it requires to monitor client or server systems.

Client Operating System Management Packs

Operations Manager 2007 supports installation of the monitoring agent on Windows 2000 Professional, Windows XP, and Windows Vista client systems. Microsoft also provides a management pack for monitoring the base operating system features of each of these operating systems. Base operating system monitoring includes availability and performance monitoring, operating system–specific views and tasks, and reports.

The extent to which an operating system can be monitored is dependent on the amount of management instrumentation included in the operating system. So an operating system such as Windows 2000 will have inherently less management instrumentation than Windows Vista and, therefore, will provide fewer objects to be monitored.

Windows Management Pack Features

Manageability has long been a part of the Windows Operating Systems. As the operating system develops more manageability features are added enhancing the ability adminsitrators have to manage the Windows environment. Windows Vista new diagnostic engine builds on the the features avaialble in Windows XP and allows great visibility into operating system to solutions such as Operations Manager 2007. Management Pack features of the Windows Management Pack are listed below. The Windows Vista specific features are noted where applicable.

Availability and Reliability

- Service Availability
- Service Failures
- Storage Availability (Vista)
- Storage Capacity Issues (Vista)
- Performance Sub-System Issues

Performance

- Shell Performance (Vista)
- Monitor Abnormalities for Key Performance Indicators (KPI) (Vista)
- Measuring for KPIs
- Operating System Startup/Shutdown Performance (Vista)

Hardware and Configuration

- Application Compatibility (Vista)
- Service Configuration Issues
- Share Configurations Issues
- Disk and Memory Failures and Issues (Vista)

Views

- Standard Views (computers, alerts, state, etc.)
- System Performance Dashboard
- Reliability Views

Tasks

- System Information
- Network Diagnostics
- System Restart/Shutdown
- Process Diagnostics

Reports (Aggregate)

- Global Reports
- Desktop Monitoring Dashboard
- Desktop Memory Report
- Desktop Disk Health Report
- Desktop Performance
- Purchasing Reports

Reports – Windows Vista-Specific

- Desktop Memory
    - Memory Failure Reporting
    - Memory Issues by RAM Type

    - Low Memory Detection
- Desktop Performance
    - System Responsiveness
    - Shell Performance by Machine and Hardware Type
    - Top Performance Issues by Type
- Desktop Disk Health
    - Disk Failures
    - Overall Disk Health
    - Disk Utilization and Capacity
- Desktop Bootup Report
    - Bootup Performance - Average Bootup Time
    - Bootup Performance - Breakdown Boot Time
- Desktop Shutdown Performance
    - Average Shutdown Time
    - Breakdown of Shutdown Time
- Disk Reliability Report
    - Machines Requiring Upgrades Across the Organization
    - Disk Failures by Drive Types
    - Disk Failure by Drive Architecture/Design
    - Disk Read/Write Failure Stats
    - Memory Failure Statistics by Type

Information Worker Management Pack

Client applications such as Internet Explorer and Microsoft Office enable information workers to be more productively. Performance problems with Information Worker applications such as these can be indicators of deeper underlying problems. Being able to monitor client applications adds an extra dimension to the visibility that Operations Manager 2007 provides IT administrators.

The Information Worker Management Pack for Operations Manager 2007 provides management capabilities for Internet Explorer 5, 6, and 7, as well as Microsoft Office 2000, XP, 2003, and Office 2007. The Information Worker Management Pack can be tuned for either Collective Health Monitoring or Business Critical Monitoring.

Information Worker Management Pack Features

Availability Monitoring

- Crash and Hang Management
- Outlook Mail Availability
- Internet Explorer Site Availability
- Data Source (Database) Availability
- File Server and File Availability

Performance Monitoring

- Resource Utilization Management

- Responsiveness Management

Advanced Monitoring Concepts

Operations Manager 2007 can be used to provide some advanced Client Monitoring scenarios, such as User Perspective monitoring or Audit Collection. User Perspective Monitoring allows IT administrators to include synthetic transactions into their end-to-end service monitoring environment. Audit Collection allows for the collection and consolidation of windows security logs from client systems.

User Perspective Monitoring (Synthetic Transactions)

Operations Manager 2007 allows creation of synthetic transactions to monitor/test availability and performance of various applications. These synthetic transactions can be as simple as pinging an IP address to determine its availability or as complicated as a series of Web transactions recorded from a browser session. The transaction returns a success or failure as well as performance data, such as time to connect. This data can be alerted on as an event or incorporated into a service to provide true end-to-end service monitoring.

Synthetic Transactions can be created for the following:

- Web Applications
- OLE DB Data Source
- TCP Port
- ASP.NET Application
- ASP.NET Web Service

Audit Collection

Operations Manager 2007 supports the collection and consolidation of Windows security log data through the Audit Collection feature. Audit Collection is supported on client operating systems running the Operations Manager 2007 agent.

Audit Collection in Operations Manager 2007 gathers all events in near-real-time as they are written to the Windows security log. The audit collection forwarding service runs on the client as a Windows Service and securely transports gathered events to the Audit Collector, which runs as an installed component on the Operations Manager Management Server. Audit Collection uses its own database so that security events—which can be voluminous in size—do not impact the scalability of the operational database used for client and server monitoring.

Audit Collection includes a Windows Management Instrumentation provider, which can be used by custom management packs to create alerts based on audit data. Several Microsoft partners are using this functionality to provide security and compliance solutions based on Operations Manager 2007 Audit Collection functionality.

Reporting is an important part of Audit Collection, and Operations Manager 2007 provides several default reports out-of-the-box.

Account Management Reports

- User account created/deleted/enabled/disabled
- Security group changes, including Administrators and Domain Admins
- Changing someone else’s password
- Computer account creation/deletion

Access Violation

- Unauthorized access attempts
- Account locked

Policy Changes

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

System Integrity

- Lost events
- Audit failure
- Log cleared

More Information

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.