

Situation

Over the years, Microsoft IT's support of line-of-business applications has evolved from mostly reactive responses to the deployment of an enterprise application monitoring solution based on System Center Operations Manager 2007. However, application availability and performance relies heavily on network devices that Operations Manager alone typically does not monitor in depth, leaving a potential gap in complete core systems monitoring and end-to-end application health visibility.

Solution

Microsoft IT has greatly enhanced its overall monitoring and support for applications and core systems by integrating EMC Smarts into its enterprise Operations Manager solution. EMC Smarts provides in-depth network device monitoring, automatic discovery, and event reporting into Operations Manager, giving a more complete view of the status of environmental components that applications rely on.

Benefits

- Reduction in administrative time and effort by consolidating two monitoring applications into a single view
- Reduction in false alarms with automated alerting, root-cause analysis, and streamlined ticket generation for network issues
- Reduction in event-to-ticket ratio
- Reduction in time to ticketing and resolution
- Ability to take proactive actions to issues before end users start calling
- Improved application service levels and increased productivity of end users

Products & Technologies

- Microsoft System Center Operations Manager 2007
- EMC Smarts Networking Suite of Products v7.0
- EMC Smarts Adapter for System Center Operations Manager 2007
- Windows Server failover clustering

Product Integration Yields Insightful Network Reporting

Published: May 2009

To effectively manage a large, complex environment, Microsoft Information Technology (Microsoft IT) has integrated EMC Smarts network monitoring into Microsoft® System Center Operations Manager 2007. The solution provides consolidated service and environment management.

Microsoft IT uses the monitoring capabilities of Operations Manager to provide insight into the availability, performance, and overall health of approximately 1,260 line-of-business (LOB) applications. More than 10,000 servers and more than 9,700 network devices with approximately 600,000 ports and interfaces deliver these LOB and other applications to more than 165,000 end users worldwide.

Operations Manager enables rich monitoring of applications, underlying services, and the server hardware components that the applications and services run on. However, Operations Manager alone does not provide comprehensive monitoring of the network and network devices that client and server applications rely on for delivery of applications to end users.

To provide a more comprehensive monitoring solution for Microsoft LOB applications and core infrastructure systems, Microsoft IT has integrated EMC Smarts into the enterprise monitoring platform. Microsoft IT implemented this integration beginning with Microsoft Operations Manager (MOM) 2000, which has added the ability to combine detailed information about network availability and performance issues with the core system and application monitoring information in Operations Manager.

The integrated solution allows for a holistic view into core systems and application availability and performance, providing a better picture of overall application and system health while enabling a streamlined approach to troubleshooting for faster issue resolution. The solution enables a smaller group of personnel to efficiently support applications and systems, and affords them the opportunity to engage in more proactive incident resolution and prevention, as opposed to reactive incident response.

This case study describes the factors in the Microsoft environment that led to the development of Microsoft IT's monitoring solution, a high-level architecture of the solution (including how Microsoft IT has integrated EMC Smarts), business benefits of the solution, and best practices for designing and operating an enterprise monitoring system based on Operations Manager with EMC Smarts integration. This case study is for enterprise application owners, chief information officers, and systems engineers responsible for designing monitoring solutions for supporting LOB applications and core infrastructure systems. It assumes that readers have a basic understanding of technologies related to network, server, and application monitoring.

Situation

Microsoft IT supports the daily IT operations of a large global corporation that has demands similar to those of many other organizations of a similar size. These demands include the requirement to provide various LOB applications for users in hundreds of locations worldwide to perform their daily work activities. LOB applications are an integral part of all areas of business at Microsoft. They facilitate strategic business planning and processes, in addition to collaboration and communication with employees, customers, partners, and vendors. With more than 1,200 LOB applications, providing the support necessary to ensure an acceptable service level for each application is a crucial component to the business of Microsoft and the charter of Microsoft IT. Supporting the needed application performance and availability service levels requires thorough monitoring of all the components of an application and the core systems that compose the IT environment.

The monitoring solution for LOB applications and core infrastructure systems at Microsoft has evolved over the years. It began as a very reactive solution based mostly on phone calls or e-mail from end users, and use of a variety of non-integrated tools, disparate network map applications, dissimilar system logs and error trap collectors, and multiple system monitoring applications with multiple consoles. These early approaches to monitoring required Microsoft IT's network operations and server operations groups to spend a great amount of time and effort manually correlating alerts from multiple systems. The additional overhead meant that Microsoft IT did not see a significant reduction in Mean Time to Identify (MTTI) or Mean Time to Repair (MTR).

Another problem was a large number of false alarms. False alarms typically are alerts from systems that appear to have a problem condition of their own. In reality, many false alarms are symptomatic events to a root cause such as a network device outage. On many occasions, the server operations team saw multiple servers go offline at once. When this happened, the server operations team typically assumed that a problem with a network device was the root cause, but the server operations engineers had to ask the network engineers to confirm the situation and provide specific details. That detailed information often involved extensive manual investigation through various tools and parsing of error logs to determine which core systems were affected and how the outage affected them. The two groups then had to manually correlate the alerts from the network and server monitoring systems to isolate root-cause events from symptomatic events, which only then enabled the teams to understand the full impact to the end-user applications. Many unnecessary ticketing (incident request) actions had to be created and subsequently closed manually because there was no single monitoring system that contained comprehensive information to programmatically generate tickets.

In addition to forcing Microsoft IT to conduct extensive research and manually correlate events and alerts from many sources, these early solutions lacked enterprise automation, consolidation, and reporting capability.

As the Microsoft monitoring product matured, Microsoft IT began to move toward a single monitoring solution that is now based on System Center Operations Manager 2007. The solution uses both the out-of-the-box and custom capabilities of Operations Manager to monitor the many LOB applications, as well as core system components such as server hardware, operating systems, and platform services like database and Web services provided by Microsoft SQL Server® database software and Internet Information Services (IIS).

Operations Manager uses management packs (MPs) to define conditions and events that are important to monitor from a server, service, or application perspective. Microsoft creates MPs for the Windows Server® operating system, SQL Server, and Microsoft Exchange products, to name a few. Nearly all Microsoft products and core server operating system services have MPs available that provide extensive monitoring capabilities specifically tailored for an application or component. These MPs are easily tuned to be relevant to a particular environment or applications so that they produce only meaningful and actionable alerts.

Operations Manager even monitors the end-user experience through synthetic transactions within custom MPs. Synthetic transactions mimic end-user activities, providing deeper insight into application service levels.

An Operations Manager–based monitoring solution enables rich monitoring of applications, platform services, and the system components that the applications and services run on. However, Operations Manager alone does not provide the depth of monitoring required for the network infrastructure, such as switches, routers, and wide area network (WAN) links. Microsoft IT lacked the combined visibility and monitoring of application, server, and network that ultimately ensures delivery of the applications to the end users. Microsoft IT needed a way to consolidate the alert stream from network events into the Operations Manager system and console to provide a single operations view into the availability and performance of applications and core systems, and to enable streamlined ticket generation and management.

Solution

Because the enterprise monitoring solution based on Operations Manager was in place and covering most components of the LOB applications and core systems at Microsoft, extending the solution to include detailed information about network conditions and events was Microsoft IT's preferred approach to provide a more comprehensive, single view into application performance and availability.

As previously mentioned, Operations Manager does not have the capability to provide comprehensive monitoring of network devices. However, Operations Manager does have the capability to integrate with other monitoring systems, either as a consumer and consolidator of incoming data from other monitoring systems, or as a provider of data to other monitoring systems.

EMC Smarts is a comprehensive network monitoring and analysis solution that integrates seamlessly into System Center Operations Manager 2007 through a product connector. The EMC Smarts Suite of products offers several network management capabilities that enhance Operations Manager, including automatic discovery of network components such as switches and routers, regardless of vendor, and it performs root-cause analysis on network service issues. The EMC Smarts Adapter for System Center Operations Manager 2007 is a fully bidirectional connector that can share information between EMC Smarts and Operations Manager. This integration of network and system management provides IT administrators and application support staff with comprehensive visibility of the end-to-end IT infrastructure through a single management console.

In the Microsoft IT solution, EMC Smarts sends root-cause alerts directly to Operations Manager. This integration of the two complementary monitoring products gives Microsoft IT a proactive solution to detect issues with core infrastructure components typically before end users begin to report problems. In most cases, Microsoft IT can commence actions to resolve

issues, or at least notify end users of an issue and expected resolution, before the users even notice an interruption in application service. The combined solution enables Microsoft IT to realize significant efficiencies in decreasing service-affecting issues.

Architecture

Integrating EMC Smarts into the enterprise monitoring solution gives Microsoft IT one network monitoring application in EMC Smarts, one system monitoring application in Operations Manager, and a single console—the Operations Manager Console—for all network, system, and application alerts. Figure 1 shows the components of the integrated monitoring solution at a high level.

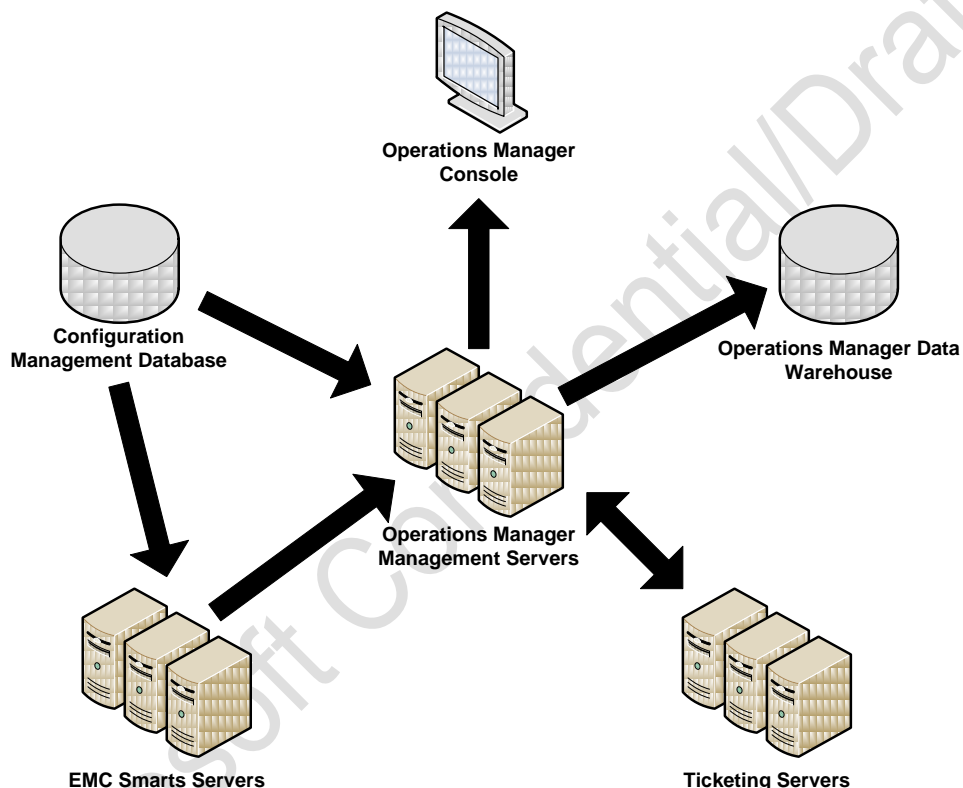


Figure 1: Microsoft IT Enterprise Monitoring System

The system consists of the following:

- **Operations Manager management servers.** Operations Manager consists of multiple management and gateway servers that manage and receive alerts from agents on monitored computers across Microsoft IT. Microsoft IT's deployment of Operations Manager consists of six management groups: three for core system monitoring of more than 13,000 agents, one for application monitoring, one for end-user experience monitoring, and one to receive the network alerts sent from EMC Smarts via the EMC Smarts Adapter for System Center Operations Manager 2007.
- **EMC Smarts servers.** EMC Smarts consists of several domain managers and adapters that all connect to a central global manager known as the Service Assurance Manager (SAM). SAM provides a single coordinated management point for all EMC Smarts

managers and adapters. Microsoft IT's deployment of EMC Smarts includes one SAM that is configured to forward alerts to Operations Manager via the EMC Smarts Adapter for System Center Operations Manager 2007.

- **Configuration Management Database (CMDB).** This repository contains information about all components in the Microsoft IT environment, including information about their relationships to LOB applications. Operations Manager and EMC Smarts consume information from the CMDB to learn about what to monitor and how it should be monitored. Microsoft IT has created an automated process that performs a daily synchronization to reconcile between EMC Smarts and the CMDB.
- **Operations Manager Console.** This is the single console that IT administrators and application support staff use to view monitoring information based on their particular role.
- **Operations Manager data warehouse.** This component stores all the alert information from each Operations Manager server for reporting purposes. Because EMC Smarts forwards alerts to one of the Operations Manager management groups, the Operations Manager data warehouse also contains all network alert data.
- **Ticketing servers.** This is the ticketing solution that Microsoft IT support staff use. The ability of Operations Manager to connect with other IT management systems, such as incident management ticketing systems, allows for automatic ticket generation based on predefined alert conditions. This ability also allows for streamlined manual ticket generation via the Operations Manager console.

Microsoft IT achieves redundancy of the overall solution by using the following fault-tolerant methods for the various solution components:

- Multiple Operations Manager management servers within each management group. Operations Manager agent failover is defined in the Active Directory® directory service, where agents can automatically discover alternate management servers.
- Failover clustering of the Operations Manager root management server. Microsoft IT has configured a two-node cluster for the root management server role.
- Multiple Operations Manager gateway servers that have been deployed in several locations to span server domains that do not share a two-way trust.
- Failover clustering of the Operations Manager SQL Server operations database and data warehouse. Microsoft IT has configured a two-node cluster for each of the SQL Server database roles.
- Mirrored EMC Smarts environments that have been deployed with both environments active but only one sending alerts at any given time to Operations Manager. Both environments are active and polling the network. Microsoft IT achieves redundancy by swapping which environment sends alerts to Operations Manager in case of failure of a component or routine maintenance such as security updates.

Benefits

Microsoft IT has realized many benefits from consolidating multiple monitoring systems into a single enterprise monitoring and ticketing solution. According a Microsoft IT operations engineer, "Consolidating the alert stream from network events into the Operations Manager system and console added a huge level of confidence knowing that alerts were correct and all in one place." The engineer goes on to say: "Since the integration of EMC Smarts, there are not many false alarms, which has greatly reduced our event-to-ticket ratio, and both

network and server operations teams have immediate correlation of what you lost, where you lost it, and what systems would be affected."

Another benefit of the integrated systems is that Microsoft IT can use the ticket-creation capabilities of Operations Manager 2007—both automatic and manual—to efficiently generate actionable tickets for network alerts. In addition to reducing the event-to-ticket ratio, the current solution greatly reduces administrative effort and time required for ticket generation, allowing subsequent corrective actions to occur more quickly and efficiently.

Microsoft IT has recognized several other important benefits by integrating EMC Smarts with Operations Manager:

- Improved application service levels has translated into increased productivity for end users.
- IT operations engineers and application support staff focus on proactive incident and problem resolution instead of reactive incident investigation.
- Consolidation of monitoring data into a single data warehouse provides comprehensive alert and performance reporting.
- EMC Smarts provides more comprehensive network monitoring and automated discovery compared to the previous network monitoring tools, including much more information about router protocol and heartbeat communications.
- The quality of the alarms has greatly increased. EMC Smarts sends only true root-cause alarms to Operations Manager. EMC Smarts understands the difference between symptomatic and root-cause events and therefore does not generate unnecessary tickets for the operations center. The result is actionable events that reduce the MTTI and MTR.
- Microsoft IT can cross-train network and server operations engineers more easily because the monitoring, ticketing, and troubleshooting systems and processes are similar.

Microsoft IT recently upgraded EMC Smarts from version 6.0 to 7.0. The team has realized the following benefits specific to that upgrade:

- Enhanced alert history logging and troubleshooting
- Overall improvement of administration tools, which has decreased manual/back-end process work
- Improved discovery mechanisms, resulting in faster device acquisition and resultant monitoring
- Reduction in time for configuration changes, from 30 minutes to 5 minutes on average
- Greatly reduced manual parsing of event logs

Future Design Improvements

Similar to an application's reliance on network devices, storage area network (SAN) fabric devices play an increasing role in overall application health. If an application has data residing on a SAN, error conditions in the SAN can greatly affect the availability or performance of the application. Microsoft IT has an extensive and growing SAN environment and is currently testing integrating Fibre Channel switch monitoring into the enterprise Operations Manager monitoring solution. This will further Microsoft IT's goal of providing a consolidated view into core infrastructure systems and application health.

Best Practices

Through implementing the integrated Operations Manager and EMC Smarts solution in such a large enterprise, Microsoft IT has developed the following best practices:

- **Monitor applications and all the platform and infrastructure components they rely on by using a single integrated solution.** Microsoft IT has realized significant benefits from integrating all monitoring into a single solution.
- **Integrate the monitoring system with the ticketing system.** Providing for automatic ticket generation and efficient manual ticket generation greatly reduces the administrative effort required to create and resolve tickets based on alerts.
- **Use Operations Manager to monitor the monitoring infrastructure.** Both Operations Manager and the EMC Smarts monitoring applications run on Windows®-based servers, and like most Windows-based applications, both Operations Manager and EMC Smarts should be monitored through an Operations Manager management pack. Microsoft IT has created a custom MP that monitors components within the EMC Smarts application to ensure that EMC Smarts alerts are all delivered to Operations Manager. Microsoft IT has created a specific rule in the MP to monitor the health of the EMC Smarts Adapter for System Center Operations Manager 2007 queue files in particular.
- **Design the Operations Manager infrastructure with scalability and redundancy in mind.** An enterprise monitoring solution is typically responsible for monitoring thousands of devices and hundreds of applications. One of the key units of scalability for Operations Manager is the management group. At Microsoft, one management group is dedicated to custom application component monitoring, while four management groups support core system monitoring of hardware, operating systems, and network monitoring alerts received from EMC Smarts. Segregating monitoring activities by management group is an effective way to meet performance and scalability requirements, and to prevent a management group from becoming a potential single point of failure for all monitoring activities. Operations Manager also provides several options for designing a fully redundant monitoring infrastructure.
- **Design the EMC Smarts infrastructure with scalability and redundancy in mind.** A network monitoring solution is typically responsible for monitoring thousands of network devices. One of the key units of scalability for EMC Smarts is the IP domain. At Microsoft, the EMC Smarts environment has been divided into 12 IP domains, and the production environment has been duplicated to provide an active/passive failover capability in case of a component outage or scheduled maintenance.

Conclusion

For several years, Microsoft IT has evolved its enterprise monitoring platform to provide a single view of the end-to-end IT infrastructure that allows for efficient and proactive support of the LOB applications that users depend on. The solution combines Microsoft System Center Operations Manager 2007 product capabilities with EMC Smarts network monitoring capabilities to provide a more holistic view into all environmental conditions and events that affect the performance and availability of applications.

Integrating EMC Smarts with Operations Manager enabled Microsoft IT to eliminate most of the effort previously spent manually correlating alerts in Operations Manager with conditions and events in the network infrastructure. With a more complete and real-time view of application health, IT administrators and application support staff can devote more time to

proactive incident and problem resolution, resulting in higher application service levels, a lower event-to-ticket ratio, and faster ticket generation and resolution.

For More Information

For more information about Microsoft products or services, call the Microsoft Sales Information Center at (800) 426-9400. In Canada, call the Microsoft Canada information Centre at (800) 563-9048. Outside the 50 United States and Canada, please contact your local Microsoft subsidiary. To access information via the World Wide Web, go to:

<http://www.microsoft.com>

<http://www.microsoft.com/systemcenter/operationsmanager/en/us/default.aspx>

<http://www.emc.com/solutions/application-environment/microsoft/solutions-for-microsoft-systems-center-operations-manager.htm>

<http://www.microsoft.com/technet/itshowcase>

© 2009 Microsoft Corporation. All rights reserved.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. Microsoft, Active Directory, SQL Server, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.