Amplify System Center
Operations Manager 2007

Managing Enterprise-Wide IT Services from a “Single Pane of Glass”

Written by
Don Jones
Co-Founder, Concentrated Technology
Microsoft MVP

White Paper
INTRODUCTION TO SYSTEM CENTER OPERATIONS MANAGER

Microsoft’s System Center Operations Manager 2007 (Operations Manager) is a powerful tool for managing IT services. Often thought of as a glorified performance monitoring tool, Operations Manager is actually much more: while it relies in part on performance information obtained from remote computers, it also focuses on data from event logs and other information to create a general “health” status for distributed applications in the environment. Rather than tying health to technological markers like processor activity or memory utilization, Operations Manager displays health information as it relates to overall system and service health.

For example, Operations Manager can display the overall health of something like “sending and receiving email,” which might encompass not only your Exchange Server, but also your internet firewall and network devices, as illustrated here:

![Figure 1. System Center Operations Manager can display the overall health of email service.](image)

But therein lies the challenge: Operations Manager can’t natively connect to the wide variety of non-Microsoft applications, clients and devices that comprise the entire health picture of your enterprise. Key software may be running on Linux servers or may rely on data from an AS/400 midrange, for example, or services may depend on network infrastructure components or even other non-Windows applications. What’s needed is a way to extend Operations Manager to non-Windows systems, effectively amplifying its capabilities by encompassing more than just Microsoft technologies.

Operations Manager also takes a knowledge-driven approach to management. Add-in management packs are written by teams with specific knowledge on how software and systems work; these teams can be key partners, the technology vendors themselves, etc. The management packs are designed to bring information into Operations Manager’s console. They roll up hundreds of performance counters, events and other information to present the health status of entire services.
THE CHALLENGE: GETTING A UNIFIED VIEW ACROSS THE ENVIRONMENT

Most IT environments today monitor their systems in vendor silos: Operations Manager might be used to monitor Windows-based systems, while other tools might be used for non-Windows systems such as Linux systems, Unix systems, Mac workstations, VMware servers, Oracle databases and Cisco devices, to name just a few. There’s nothing technically wrong with this approach, and in fact there can be excellent reasons to choose it, including the reality that these disparate systems are often managed by different professionals who are comfortable with different tools and who have different skill sets.

From a management perspective, however, splitting up monitoring can have devastating effects. Consider an example:

Joe helps manage his organization’s Windows-based infrastructure. Operations Manager informs him that the organization’s ability to send email to and from the internet is diminished due to connectivity issues. Because Joe doesn’t manage the firewall, he passes the problem to Marty, who works in the organization’s networking team. Marty runs some tests against the firewall and concludes that it’s working perfectly, so he tosses the problem back to Joe.

While these two argue, the real issue resides in the Linux-based DNS server, which is experiencing hardware problems and isn’t answering name resolution queries promptly. Of course, that machine is run by Alice, who works in the organization’s Linux/Unix management division.

All three of these professionals have the right tools to manage their systems, but nobody’s looking at the whole environment. Therefore, problems get passed around until someone feels like dealing with them, or until there’s a critical outage that impacts a service-level agreement (SLA) or operations-level agreement (OLA), resulting in downtime, user complaints, lost money and missed business opportunities, and upset managers and executives.

The problem with the silo approach, in a nutshell, is that problems frequently don’t get fixed until they’re blazing fires, rather than being caught before they cause a negative impact. What’s needed is a way to have one centralized view to look at the entire environment from the perspective of your mission-critical systems and services, with an understanding of all the dependencies and the means to examine those dependencies for problems. System Center Operations Manager is the perfect tool for meeting this need—but it needs some help.
Figure 2. Operations Manager provides end-to-end service views in your Windows environment.

THE SOLUTION: OPERATIONS MANAGER EXTENSIONS

Quest Software amplifies Operations Manager by extending its capabilities to additional non-Windows systems and infrastructure.

Quest Management Extensions for Operations Manager 2007 (QMX) extends Operations Manager to Oracle, Cisco, VMware, RedHat and other systems with a significant library of 250+ agentless management packs. These management packs integrate directly into Operations Manager and range across “categories” such as:

- Operating systems (non-Windows)
- Applications
- Network
- Databases
- Infrastructure
- Storage
- Security
- Mid-range and Mainframes
- Power
- Telecom
Amplify System Center Operations Manager 2007

- Virtualization
- Hardware

For a complete list, visit: http://www.quest.com/QMXSupportedPlatforms.

Standards-based Architecture

QMX uses the Web-Based Enterprise Management (WBEM) and Common Information Model (CIM) standards used natively in Operations Manager, exposing information about non-Windows systems through Windows Management Instrumentation (WMI) interfaces. Management rules for non-Windows systems are thus configured in exactly the same way as Windows systems—without modifying the base Operations Manager product.

Imagine the Management Possibilities

With Operations Manager and QMX, administrators are no longer stuck in technology silos. Instead, they can focus on the entire picture and provide true end-to-end IT service management. Let’s revisit our earlier example and see how it would play out with QMX in the picture:

Joe receives an alert from Operations Manager that the organization’s ability to send email to the internet is becoming degraded. He immediately opens the Operations Manager console and reviews the situation. He can see that internet connectivity is fine, but that one of the Exchange Server’s dependencies is the Linux-based DNS server, which is intermittently failing to respond to name resolution requests. Joe uses Operations Manager to conduct a quick interactive test of the DNS server and sees several requests time out. He immediately contacts Alice, who is responsible for the organization’s Linux and Unix machines, and alerts her to the problem.

Alice tells Joe that she already has someone working on the problem: Operations Manager had sent her an email as soon as it detected that the DNS server’s response times were increasing.

Alice’s team fixes the problem, restoring full capability to the various systems and services that depend upon the Linux server. All of this happens without email or any other service becoming unavailable—thus avoiding an outage that may have cost the company a great deal. In fact, most users are unaware that a problem even occurred.

Because QMX allows Operations Manager to include non-Windows systems and devices as “first-class citizens”, and shows the service dependencies between all of the components in the environment, administrators can more easily identify trouble spots, dispatch the appropriate resources to fix them, and in many cases avoid production impact entirely by reacting to degrading conditions through Operations Manager alerts.
Figure 3. QMX extends the reach of Operations Manager to include non-Windows systems and components.

**Complete Capabilities**

QMX enables the full range of Operations Manager capabilities for supported non-Windows devices, including:

- Automated health alerts
- Management rules determining when something is considered “healthy” or not
- Performance monitoring
- Health and performance reporting
- Full integration with Microsoft’s Audit Collection Services (QMX brings non-Windows security event log files into ACS), helping to achieve and maintain compliance with legal and industry requirements
- Windows scripting, to further extend non-Windows monitoring and automation with no need for intimate knowledge of Unix or Linux scripting
- Event collection, by turning lines from syslog or regular log files into Operations Manager events
Respecting Boundaries

Quest realizes that many administrators of non-Windows systems aren’t eager to install agents and software on their systems, and are concerned that they’re “turning over” management of their systems to “others” running Operations Manager. Nothing could be further from the truth with QMX! QMX uses agentless extensions, meaning nothing is installed on the monitored systems and devices.

Moreover, using QMX and Operations Manager doesn’t preclude the use of other, existing monitoring tools; administrators of non-Windows systems can continue monitoring their systems just as they always have. The only change will be that an additional monitoring tool, Operations Manager, will be keeping an eye on things and aggregating data into a truly enterprise-wide view of the systems and services provided to end users.

Quest does provide software agents for advanced management points, such as .NET Framework applications, giving you the option of using a more distributed architecture and gaining additional management features.

Completely Secure

Because QMX uses an agentless architecture to extend Operations Manager, QMX obviously needs to store login user names and passwords for the non-Windows systems it helps Operations Manager monitor. QMX secures these credentials through standards-based RSA encryption, and also supports SSH and public/private key authentication. These features are all designed to help you maintain a centrally managed, safe and secure operating environment.

Connect to More

As previously mentioned, Quest offers select agent-based Management Packs to help unite Operations Manager with even more non-Microsoft management platforms (where leveraging an agent makes the most sense architecturally). You can choose from:

- Quest Management Pack for AS/400
- Quest Management Pack for z/OS
- Quest Management Pack for .NET

The Quest Management Pack for .NET, to highlight one of the listed, enables Operations Manager to monitor .NET Framework applications for exceptions, proactively alert IT resources when problems occur, and seamlessly integrate IT operations with development workflows, helping to accelerate time to resolution by support teams. This Management Pack also helps eliminate the need for your .NET developers to spend time solving production problems, giving them more time to be developers.
Many organizations have already invested heavily in a variety of management tools (or have written custom scripts) that may or may not include Operations Manager. If Operations Manager serves as the “single pane of glass,” most third-party management frameworks can be integrated with Operations Manager via a host of bi-directional connectors provided by Quest. And if you choose to have another framework server as the “manager of managers,” you can still leverage the ability of Operations Manager and QMX to manage both Windows and non-Windows elements in your environment and feed needed data into your enterprise management platform of choice.

The Quest Management Connectors (QMC) allow more than 20 enterprise management platforms to be integrated with the alert, event and performance data collected by Operations Manager. This integration enables administrators to use their preferred “single pane of glass” while still taking advantage of the robust, service-level monitoring and alerting provided by Operations Manager and QMX.

Supported management platforms include the following platforms, and many more:

- CA UniCenter
- HP OpenView
- Oracle Enterprise Manager
- BMC (Remedy, Patrol and Magic)
- SolarWinds
- Spectrum
- IBM Tivoli
- HP Insight Manager
- Quest Foglight
- Quest Big Brother

Figure 5. QMC allows 20+ enterprise management platforms to be integrated with the data collected by Operations Manager and vice versa.
ONE ENTERPRISE. ONE VIEW. MANY ADVANTAGES.

Operations Manager and QMX give your organization the holistic view of your enterprise services and systems that it needs. With these powerful tools working together, you can:

- Define and meet end-to-end service level agreements (SLAs)
- Troubleshoot and resolve system issues quickly
- Assign problems to the technology team best equipped to solve them
- Deal with issues before they have a negative impact on your production environment
- Streamline your support processes and eliminate “back-and-forth blame” between support teams

QMX allows Operations Manager to cover all of the dependencies in your enterprise services. You no longer need to manage “as much as you can” from Operations Manager and turn to other tools and scripts for the rest—a strategy that promotes disparate management, guesswork and manual troubleshooting. Instead, with QMX, services can encompass both Windows-based and non-Windows servers, network devices, database management systems, storage solutions, mainframes, security devices and much more.

With QMX, you can use Operations Manager to produce management reports that reflect the entire enterprise picture. Here are some of the challenges you’ll be able to address:

- Not meeting your SLAs or OLAs? Operations Manager and QMX can show you exactly which enterprise components are contributing to the problem—without weeks of research and hand-wringing by technology teams seeking to pass the blame to someone else.
- Need to review your technology budgets? Operations Manager and QMX can show exactly which enterprise components are working at maximum capacity and may be due for an upgrade—based on production data rather than guesswork. Furthermore, using Operations Manager in this manner maximizes the investment you’ve made and may help you reduce the number of tools required to manage your infrastructure. Struggling with legislative or industry requirements that demand service availability (such as Gramm-Leach-Bliley)? With QMX, Operations Manager can help spot problems before they become fires, by carefully and automatically watching everything that can impact availability.
• Already invested in an enterprise management platform like OpenView, UniCenter, or Tivoli? Now you can either integrate all of your systems by having that system feed Operations Manager, or enable that platform by feeding it end-to-end information about the state of your environment, through the QMC. Use Operations Manager and QMX to do the heavy lifting, and then connect all of that data to whatever “single pane of glass” your technologists prefer.

With its QMX and QMC offerings, Quest Software amplifies Operations Manager by enabling a single enterprise view of production services from a single management solution.
ABOUT THE AUTHOR

Don Jones is a co-founder of Concentrated Technology (ConcentratedTech.com). His consulting practice specializes in making the connection between technology and business, helping businesses realize more value from their IT investment, and helping IT align more closely to business needs and values. Don is also a Microsoft “Most Valuable Professional” (MVP) Award recipient, and the author of more than 30 books on information technology. He has been an IT journalist for more than eight years, and is currently a contributing editor for Microsoft TechNet Magazine. Don is a sought-after speaker at industry conferences and symposia, including Connections conferences, Microsoft TechEd and TechMentor events.
ABOUT QUEST SOFTWARE, INC.

Quest Software, Inc., a two-time winner of Microsoft’s Global Independent Software Vendor Partner of the Year award, 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. Quest’s Windows management solutions simplify, automate secure and extend Active Directory, Exchange Server, SharePoint, SQL Server, .NET and Windows Server as well as integrating Unix, Linux and Java into the managed environment. Quest Software can be found in offices around the globe and at www.quest.com.

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