

Every device, every operating system and every user action generates machine data with latent value that can be used to inform IT strategic planning and operational insight. First, however, IT administrators must figure out how to collect, manage and consume the data.

How does log analytics in OMS simplify this challenge?

Operations Management Suite, includes an analysis service that enables IT administrators to gain deep insight into their environments. OMS enables customers to interact with real-time and historical machine data to rapidly develop custom insights, and powerful search capabilities that enable ad-hoc root cause analysis and automated troubleshooting across multiple data sources.

Without instrumenting any code directly or having knowledge of any complex schema, IT admins quickly receive interactive results. Integrated search enables customers to drill deeper into areas of interest that are highlighted by Solution Packs, and provides Microsoft and community-developed patterns for analyzing data. Search also enables customers to form their own hypotheses and query the data to find custom insights through proactive exploration or reactive troubleshooting.

The right tool for the right job

OMS enables operations teams to collect and analyze machine data from virtually any source – regardless of volume, format or location. This enables customers to get the benefits of all their data, whether located in datacenters, the public cloud, physical or virtual. OMS can consume the data and provide a single, intuitive and powerful experience. Making it easy for system administrators to quickly realize operational value.

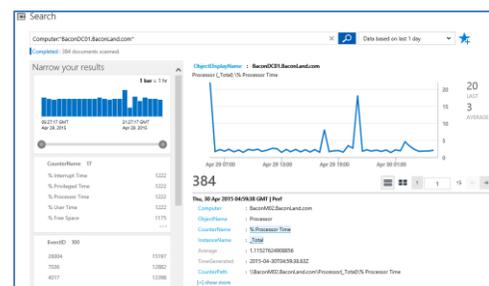
Built-in intelligence

OMS with inbuilt log analytics provides proactive operational data analysis through the delivery of Solution Packs. Solution Packs can be selected from an integrated gallery and offer pre-built rules and algorithms that perform initial analysis for critical scenarios like capacity planning, configuration intelligence and change tracking. Microsoft provides intelligence packs based on learnings gathered from operating cloud-scale datacenters. Making it easy for system administrators to quickly realize operational value by:

- **Search and investigate** – helps you to search for key words, values and fields in seconds, enabling to uncover valuable and actionable insights throughout your infrastructure.
- **Custom Dashboard and views** – create dashboard by choosing different chart visuals and setting your own thresholds
- **Capacity planning** - get deep visibility into your data center capacity, investigate “what-if” scenarios, identify stale and over-allocated virtual machines, and plan your future compute and storage needs.

Key benefits

- Works with any platform, on any cloud – AWS or Azure, Windows Server or Linux, OpenStack or VMware
- Ready-made intelligence for common IT tasks
- Real-time central data repository
- Rich dashboard and reporting capabilities powered by search queries
- Reduce infrastructure and maintenance costs
- Supports multiple devices and users



Microsoft Operations Management Suite



Inbuilt log analytics to unleash operational intelligence

- **Update status** - identify missing system updates across all of your servers whether they're running in your data center or in a public cloud.
- **Change Tracking** - when you troubleshoot an operational incident, the first thing you want to know is what has changed on your servers. Log analytics helps to easily identify operational issues caused by software changes that occur in your environment.



- **Detecting security breaches** – enabling an efficient, scalable and secure way to collect and store security records. The robust search capabilities provides the ability to easily answer the question of who did what, when and on which devices.
- **Security log collection for auditing** - helps Security Analyst and System Admins to mine large distributed sets of security data in order to detect suspicious activities and potential security breaches.

How does it work?

If you are an existing System Center customer you can onboard your Operations Manager management groups to Operational Management Suite via the Operations Manager console. On-premises and Azure resources can also send data directly to the service using the Microsoft Monitoring agent directly. Whether you're in the public cloud, on-premises or have a hybrid solution, OMS can provide the best options for you giving you greater flexibility. Learn more about onboarding at www.microsoft.com/oms.

Enhancing your System Center investments

Operations Management Suite enhances your System Center investments through integration with what you have today. Extending this capability through many new and enhanced scenarios including:

Proactive smart alerts	Security Log Collection
Comprehensive operations dashboards, and reporting	Breach and Threat detection
Real-time and customizable monitoring	Deep forensic analysis
Customizable dashboards	Malware detection and Software update status
Monitoring of OS Resources (CPU, disk, memory, network) for Windows, Linux systems	Detect potential configuration issues or deviations from identified best practices.
On-premise server performance monitoring	Adding structure to all types of unstructured data
Azure server performance monitoring	Real-time monitoring, search and log analytics
SAN Storage analytics	Dashboards powered by search queries
Forecast resource utilization trends	Third party and community based intelligence packs
Optimize virtual machine placement, investigate "what-if" scenarios, pinpoint capacity shortages and identify stale and over-allocated VMs	Monitor Software, Windows Services, Registry Keys, Group Policy and File changes
Identify storage bottlenecks	Universal log collection and analysis

Let's get started today Join us today by visiting <http://www.microsoft.com/oms> and try it for free.